FEDERAL BUREAU OF INVESTIGATION | COUNTERTERRORISM DIVISION

Joint Terrorism Task Force

Task Force Officer Orientation

A reference guide for new JTTF Task Force Officers

Volume 1
Revision 1
December 2009

TABLE OF CONTENTS

F O R E W A R D

The mission of the National Joint Terrorism Task Force, and the NJTTF's vision for the more than 100 JTTFs nationwide, is to enhance communications, coordination and cooperation between federal, state, and local government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety and homeland security community by providing a point of fusion for terrorism intelligence and investigations.

As a Task Force Officer (TFO), you represent an indispensable asset to JTTFs and the FBI as a whole. Your specialized training and localized expertise represent a window into your community that could not be duplicated by any government department. Together with the FBI and the participating agencies of your JTTF, you will provide resources and regional proficiency that ensure the safety of the United States, your state, your neighborhood and your family and friends.

This orientation manual is provided to assist your transition from local, state, or federal official to JTTF Task Force Officer. We anticipate that your time with the JTTF will be rewarding, and trust that your presence will greatly contribute to the mission of the FBI Counterterrorism Division. Thank you for your service.

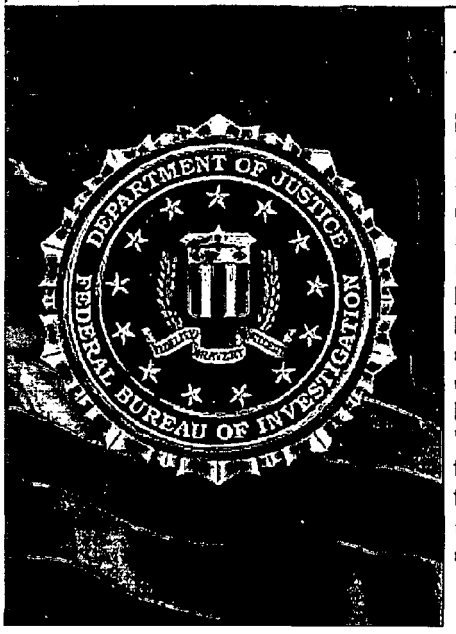
Michael J. Heimbach

Michael J. Heimbach

Assistant Director
Counterterrorism Division

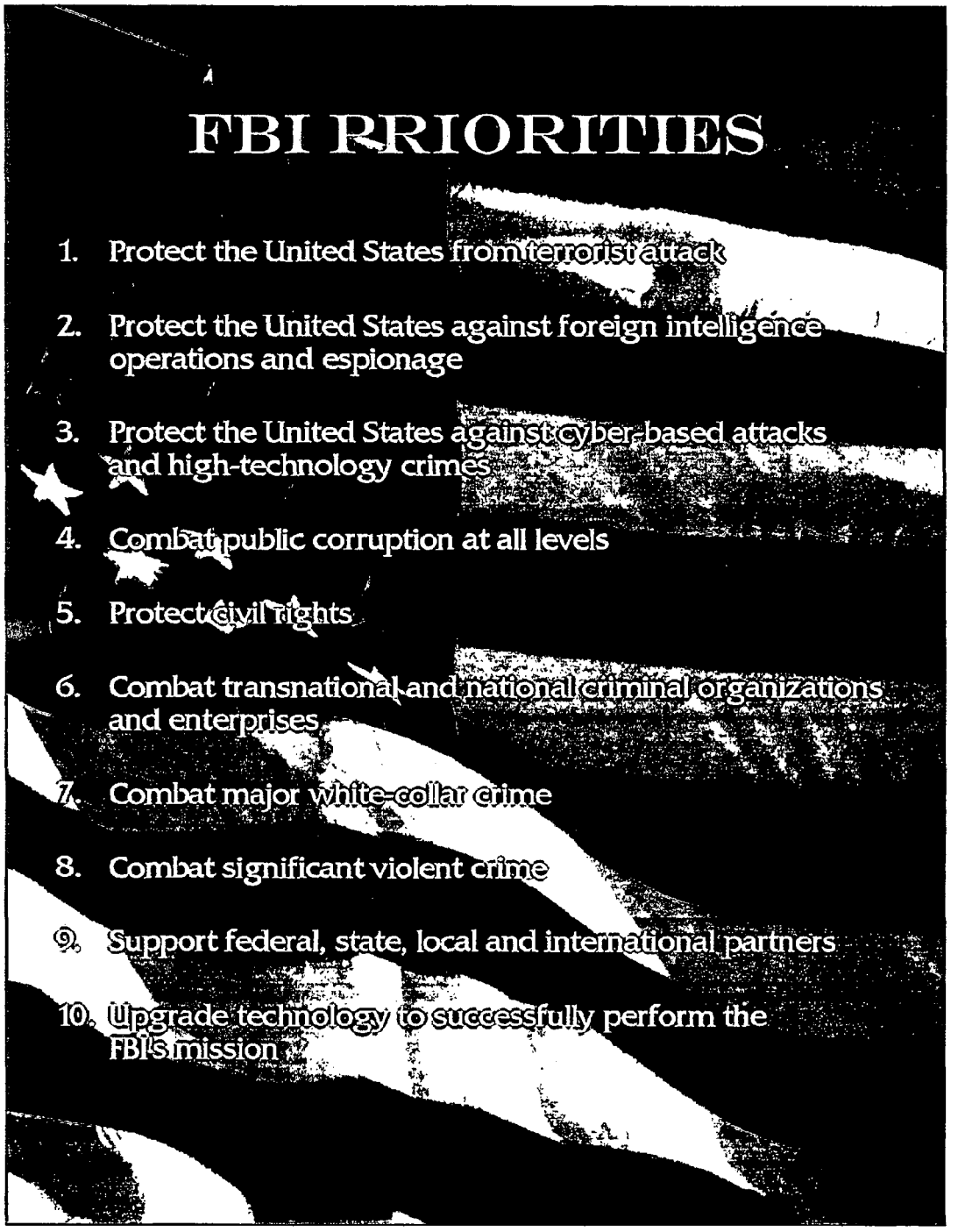
Justice

Heraldry of the FBI Seal



The actual FBI Seal is in color and was adopted in 1940.

Each symbol and color in the FBI Seal has special significance. The dominant blue field of the Seal and the scales on the shield represent justice. The circle of 13 stars denotes unity of purpose as exemplified by the 13 original states. The laurel leaf symbolizes academic honors, distinction, and fame. There are 46 leaves in the two branches, since there were 46 states in the Union when the FBI was founded in 1908. Red parallel stripes stand for courage, valor, and strength, while the white stripes convey cleanliness, light, truth, and peace. As in the American Flag, the red bards exceed the white by one. The motto, "Fidelity, Bravery, and Integrity," describes the motivating force behind the FBI. The peaked bevelled edge surrounding the Seal symbolizes the challenges facing the FBI and the ruggedness of the agency, and the gold color in the seal conveys its overall value.


FBI PRIORITIES
1. Protect the United States from terrorist attack
2. Protect the United States against foreign intelligence operations and espionage
3. Protect the United States against cyber-based attacks and high-technology crimes
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational and national criminal organizations and enterprises
7. Combat major white-collar crime
8. Combat significant violent crime
9. Support federal, state, local and international partners
10. Upgrade technology to successfully perform the FBI's mission

THUMBNAIL HISTORY OF THE FBI

On July 26, 1908, Attorney General Charles J. Bonaparte ordered a small force of permanent investigators (organized a month earlier) to report to the Department of Justice's Chief Examiner, Stanley Finch. All Department of Justice [DOJ] investigative matters except certain bank frauds, Bonaparte declared, were to be reported to this new group of detectives for handling. At first, little seemed to come of Bonaparte's reorganization. In fact, this small special agent force evolved into the FBI, the primary federal law enforcement agency in the United States.

In 1909, this agent force was named the Bureau of Investigation [BOI]. At this time, it investigated antitrust matters, land fraud, copyright violations, peonage, and twenty other matters. Over the next decade, federal criminal authority and Bureau jurisdiction were extended by laws like the 1910 "White-Slave Traffic" Act that put responsibility for interstate prostitution under the Bureau for a time and the 1919 Dyer Act that did the same for interstate auto-theft. U.S. entry into WWI in April 1917 increased the Bureau's jurisdiction too. Congress and President Wilson assigned the BOI's three hundred employees responsibility for espionage, sabotage, sedition, and selective service matters.

Rising prosperity and a growing criminal threat characterized the 1920's. With the advent of the automobile and Prohibition, bank robbers, bootleggers, and kidnapers crossed state lines to elude capture because of jurisdictional boundaries. A flourishing criminal culture marked by violent gangsters arose as no federal law gave the BOI authority to tackle their crimes and other law enforcement efforts were fragmented. The Bureau addressed these matters as its jurisdiction permitted throughout the 1920's.

In 1924, Attorney General Harlan Stone appointed John Edgar Hoover as Director. Director Hoover [1924-1972] implemented a number of reforms to clean up what had become a politicized Bureau under the leadership of William J. Burns [1921-1924]. Hoover reinstated merit hiring, introduced professional training of new agents, demanded regular inspections of all Bureau operations, and required a strict professionalism in the Bureau's work.

Under Hoover, the Bureau also began to emphasize service to other law enforcement agencies. The Identification Division was created in 1924 to provide U.S. police a means to identify criminals across jurisdictional boundaries. The Technical Crime Laboratory, created in 1932, provided forensic analysis and research for law enforcement, and the FBI National Academy, opened in 1935, provided standardized professional training for America's law enforcement communities.

In answer to the violent crime of the 1930's, Congress began to assign and expand new authorities to the Bureau. The kidnapping and murder of the Lindbergh baby in 1932 led to the passage of the Federal Kidnapping Act, which allowed the Bureau to

investigate interstate kidnappings. The 1933 Kansas City Massacre spurred the passage of the 1934 May/June Crime Bills. These laws gave the Bureau authority to act in many new areas, to make arrests, and to carry weapons. Renamed "Federal Bureau of Investigation" in 1935, the FBI dealt with gangsters severely, earning its anonymous agents the sobriquet of "G-Man."

As the gangster threat subsided, a threat of a different nature emerged. In 1936, President Roosevelt directed the FBI to investigate potential subversion by Nazi and Communist organizations. In 1940, he tasked the Bureau with responsibility for foreign intelligence in the western hemisphere and domestic security in the United States. In response, the Bureau created a Special Intelligence Service [SIS] Division in June 1940. The SIS sent undercover FBI Agents throughout the Western Hemisphere. These Agents successfully identified some 1,300 Axis intelligence agents [about 10% of whom were prosecuted]. When President Truman ordered the program's end in 1947, several former SIS offices became the backbone of the FBI's foreign liaison efforts, now serving as Legal Attaché Offices [Legat Offices]. FBI efforts also thwarted many espionage, sabotage, and propaganda attempts on the home front including Frederick Duquesne's spy ring in 1941 and George Dasch's band of saboteurs in 1942.

When Germany and Japan surrendered in 1945, concern about the threat of foreign intelligence did not end. Revelations that year from former Soviet intelligence agents like Igor Guzenko and Elizabeth Bentley, information gleaned from FBI investigations during and after the war, and decrypted/decoded Soviet cable traffic called "Venona" [available to the Bureau from 1947] convinced the FBI of the seriousness of the Soviet intelligence threat long before Senator Joseph McCarthy made his 1950 speech about communist "moles." Under the Hatch Act [1940] and Executive Orders issued in 1947 and 1951, the Bureau exercised responsibility for ensuring the loyalty of those who sought to work in the government. The FBI played a critical role in U.S. handling of the Cold War.

In the 1950's, civil rights violations and organized crime became matters of increasing concern. As in the past, lack of jurisdiction hindered the Bureau from effectively responding to these problems when they first emerged as national issues. It was under the 1964 Civil Rights Act and the 1965 Voting Rights Act that the Bureau received legislative authority to investigate Civil Rights violations. Under existing laws, the Bureau's efforts against organized crime also started slowly. Then, with the 1968 Omnibus Crime Control and Safe Streets Act and the1970 Organized Crime Control Act, Congress gave the Bureau effective weapons with which to attack organized criminal enterprises, Title III warrants for wiretaps and the Racketeering and Corrupt Organizations Act [RICO].

During the 1960's, subversion remained a central focus of Bureau efforts. The counter-cultural revolution turned the Bureau's attention towards violent student movements as criminal groups like the Weather Underground and the Black Panthers engaged in both legitimate political action and illegal crime. The Bureau responded to

the threat of subversion with Counterintelligence Programs, COINTELPRO, first against the Communist Party [1956], later against other violent/subversive groups like the Black Panthers and the Ku Klux Klan [1960's].

During the 1970's, Bureau actions, which were publicly revealed through a strengthened Freedom of Information Act [1966, amended in 1974], resulted in congressional investigations like the Church Committee and the Pike Committee hearings in 1975. In response to criticisms emerging from these revelations, the Bureau worked with Attorney General Levi to develop guidelines for its domestic counterintelligence investigations.

In the wake of Director Hoover's death in May 1972, Director Clarence M. Kelley [1973-1977] refocused FBI investigative priorities from the quantity of results to the quality of cases handled. Working with the Bureau and Congress in 1976, Attorney General Edward Levi issued a set of investigative guidelines to address the concerns of Bureau critics and to give the FBI the confidence of having public, legal authority behind its use of irreplaceable investigative techniques like wiretaps, informants, and undercover agents. These investigative techniques were used to great effect in cases like ABSCAM [1980], GREYLORD [1984], and UNIRAC [1978]. In 1983, as concerns about terrorist acts grew, Attorney General William French Smith revised the Levi Guidelines to adjust the Bureau's ability to prevent violent radical acts.

Director William H. Webster [1977-1987] built upon Director Kelley's emphasis on investigative "quality" cases by focusing Bureau efforts on three Priority Programs - White Collar Crime, Organized Crime, and Foreign Counterintelligence. Later Illegal Drugs [1982], Counterterrorism [1982], and Violent Crimes [1989] were identified as priority programs too. This concentration of resources brought great success against Soviet and East Bloc intelligence as more than 40 spies were arrested between 1977 and 1985. The FBI also made breakthroughs against white-collar crime in investigations like ILLWIND [1988] and LOST TRUST [1990], and in organized crime cases like BRILAB [1981] and the PIZZA CONNECTION [1985].

During the 1990's, criminal and security threats to the United States evolved as new technology and the fall of communism in the Soviet bloc changed the known geopolitical world. The 1993 bombing of the World Trade Centers and the 1995 bombing of the Oklahoma City federal building highlighted the potentially catastrophic threat of both international and domestic terrorism. The FBI responded to the emerging international face of crime by aggressively building bridges between U.S. and foreign law enforcement. Under Director Louis J. Freeh [1993-2001], the Bureau expanded its Legat Program [39 offices by fall-2000]; provided professional law enforcement education to foreign nationals through the International Law Enforcement Academy [ILEA] in Budapest [opened in1994] and other international education efforts; and created working groups and other structured liaisons with foreign law enforcement.

The Bureau also strengthened its domestic agenda. Responding to criticism of its actions in the 1993 standoffs at Waco, Texas, and Ruby Ridge, Idaho, the Bureau revamped its crisis response efforts. The FBI's commitment to law enforcement service was strengthened by the computerization of its massive fingerprint collection database, enhancements in the National Crime Information Center [NCIC] and in NCIC 2000, and by the revitalization of the FBI Laboratory. In 1997, the Bureau hired its first professional scientist to head the Lab. The Lab

tightened its protocols for evidence control, instituted organizational changes to optimize research specialization, and earned national accreditation.

On September 4, 2001, former U.S. Attorney Robert S. Mueller III [2001 to present] was sworn in as Director with a mandate to address a number of steep challenges: upgrading the Bureau's information technology infrastructure; addressing records management issues; and enhancing FBI foreign counterintelligence analysis and security in the wake of the damage done by former Special Agent and convicted spy Robert S. Hanssen.

Then within days of his entering on duty, the September 11 terrorist attacks were launched against New York and Washington. Director Mueller led the FBI's massive investigative efforts in partnership with all U.S. law enforcement, the federal government, and our allies overseas. On October 26, 2001, the President signed into law the U.S. Patriot Act, which granted new provisions to address the threat of terrorism, and Director Mueller accordingly accepted on behalf of the Bureau responsibility for protecting the American people against future terrorist attacks. On May 29, 2002, Attorney General John Ashcroft issued revised investigative guidelines to assist the Bureau's counterterrorism efforts.

To support the Bureau's change in mission and to meet newly articulated strategic priorities, Director Mueller called for a reengineering of FBI structure and operations that will closely focus the Bureau on prevention of terrorist attacks, on countering foreign intelligence operations against the U.S., and on addressing cyber crime-based attacks and other high technology crimes. In addition, the Bureau remains dedicated to protecting civil rights, combatting public corruption, organized crime, white-collar crime, and major acts of violent crime. It is also strengthening its support to federal, county, municipal, and international law enforcement partners. And it is dedicated to upgrading its technological infrastructure to successfully meet each of its priorities.

At the start of the new millennium, the FBI stands dedicated to high values and ethical standards. Commitment to these values and standards ensures that the FBI effectively carries out its mission: Protect and defend the United States against terrorist and foreign intelligence threats; uphold and enforce the criminal laws of the United States; and provide and enhance assistance to its federal, state, municipal, and international partners.

Ever wonder how the FBI got its name?

It's more confusing than you might think.

First, it had no name. In 1908 when Attorney General Charles Bonaparte created the entity that would become the FBI, he did not name it. He simply referred to the group as a "special agent force" when he announced his work to Congress in the 1908 Attorney General's Annual Report.

Second, it was named the Bureau of Investigation but, sometimes, called the Division of Investigation. In 1909, Attorney General Wickersham formally named Bonaparte's "force" the Bureau of Investigation [BOI]. At the time, the Bureau was composed of less than seventy employees. Over the next several years the Bureau was also referred to as the Division of Investigation, but this title did not stick. Between 1913 and 1933, the Bureau remained the Bureau of Investigation. In 1933 it was named the United States Bureau of Investigation.

Third, and most confusingly, the Bureau became the Division of Investigation. In the spring of 1933, newly elected President Franklin Roosevelt reorganized the Department of Justice [DOJ]. This reorganization grew out of the end of Prohibition: In 1919, the 18th Amendment had been passed, outlawing the sale and manufacture of alcohol and enforced by the Treasury Department's Bureau of Prohibition [BOP]. In 1929, the BOP was transferred to the DOJ from the Treasury Department. But what does this have to do with the FBI?

Well...in June of 1933, President Roosevelt ordered the formation of a Division of Investigation composed of the Bureau of Investigation and the Bureau of Prohibition. Director Hoover was appointed as Director of Investigation but also remained Director of the BOI. The leadership of the BOP was left largely to John S. Hurley as Assistant Director in charge of the BOP. Hoover maintained a stark separation between the two Bureaus and he refused to integrate BOP personnel into the BOI. [For more on this confusing period, see the "Byte Out of History on Elliot Ness and the Bureau."]

In the fall of 1933, the 18th Amendment was repealed and the Bureau of Prohibition withered and died. Its enforcement functions were ended so its Agents were transferred or fired; a very small number became FBI Agents. BOP property was transferred throughout the government (we kept a lot of cars, most of the boats and airplanes went to other departments) and its tax law enforcement authority was transferred back to Treasury. The few remaining enforcement functions related to crimes committed under the old prohibition laws were handled by the Division of Investigation.

Finally, the FBI. By default, the Bureau of Investigation had become the Division of Investigation. This was confusing as there were several "Divisions of Investigation" in the federal government at that time. Director Hoover, therefore, asked

that his Division be given a distinctive name. Attorney General Cummings broached the issue with President Roosevelt and Congress and they agreed. In the 1935 the Department of Justice appropriation, Congress officially recognized the Division as the Federal Bureau of Investigation, the FBI. Almost immediately, Inspector W. Drane Lester coined the FBI's motto - Fidelity, Bravery, and Integrity. It was quickly adopted and published in The Investigator for all Bureau employees to see. The name became effective on March 22, 1935, when President Roosevelt signed the appropriation bill. We have been known under this distinguished name ever since.

Where did the title "Special Agent" come from?

The bottom line: no sources say why the term "special agent" was first used in the 1870's by the Department of Justice, only that it was used...and evolved into today's FBI Special Agent.

Here are the facts:

In 1870, after Congress appropriated $50,000 for the detection and prosecution of crimes, Attorney General George Williams appointed a "special agent" in the Department of Justice and paid him with monies from this appropriation. This agent conducted "special" investigations for the Attorney General, i.e. the Attorney General assigned which cases his agent was to investigate. Other government law enforcement agencies may have also used a similar title from time to time, but none used it for an extended period of time.

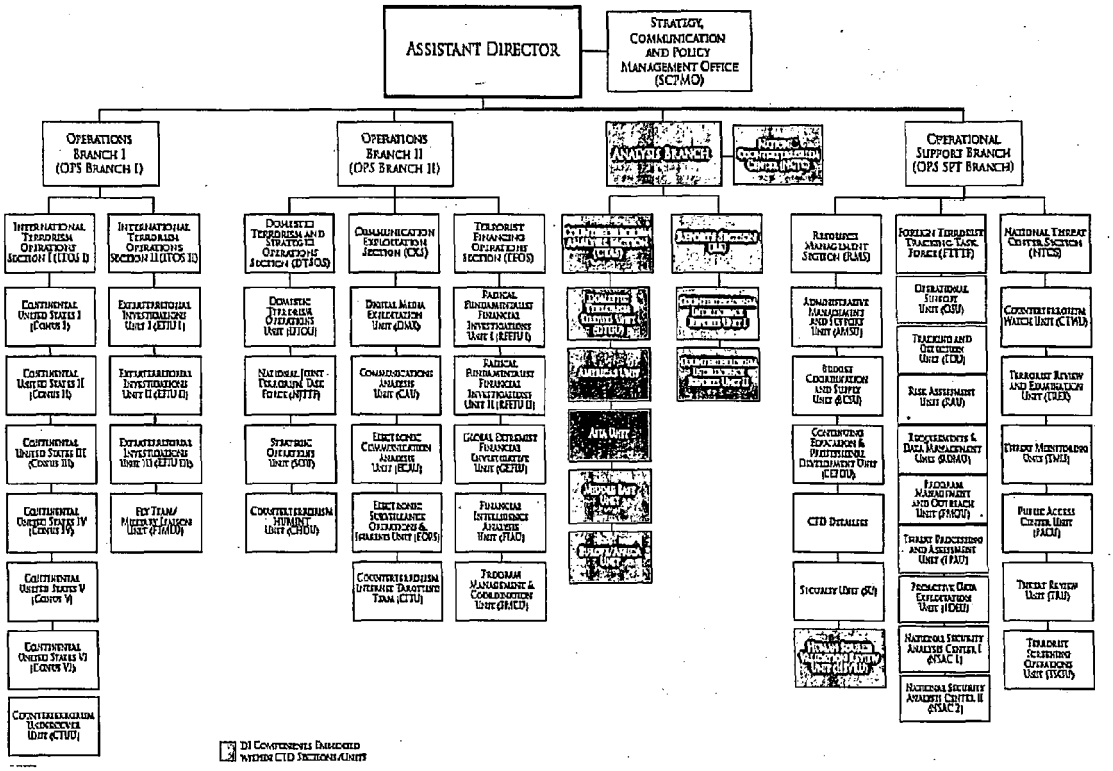
By 1879, the DOJ title was changed to General Agent, a supervisory role [this position was abolished in 1907]. In 1894 a "special agent" was assigned to work under the General Agent, investigating violations of the Indian Intercourse Act. The bulk of Department investigations between 1879 and 1908 were handled by Secret Service personnel who were borrowed on a case-by-case basis. In 1907, the year before the Bureau of Investigation (the FBI's precursor) was created, one DOJ special agent investigated antitrust matters, one handled investigations related to the Government's defense of suits before the Spanish Treaty Claims Commission, and one special agent handled Indian Intercourse Act violations.

In 1908 when Attorney General Charles Bonaparte reorganized the Department's investigators into a "special agent force," he hired 9 Treasury agents as special agents and put them together with 13 peonage investigators, and 12 bank examiners. Whether all or some of the peonage investigators were called special agents is not known. The bank examiners were accountants and were usually called "special examiners." A distinction immediately arose between special agents and special accountants. This distinction existed into the 1930's; at which point, it was decided that all investigative agents--agents and accountants--were to be called Special Agents. It was around this time that the convention of capitalizing "Special Agent" became uniform in the Bureau.

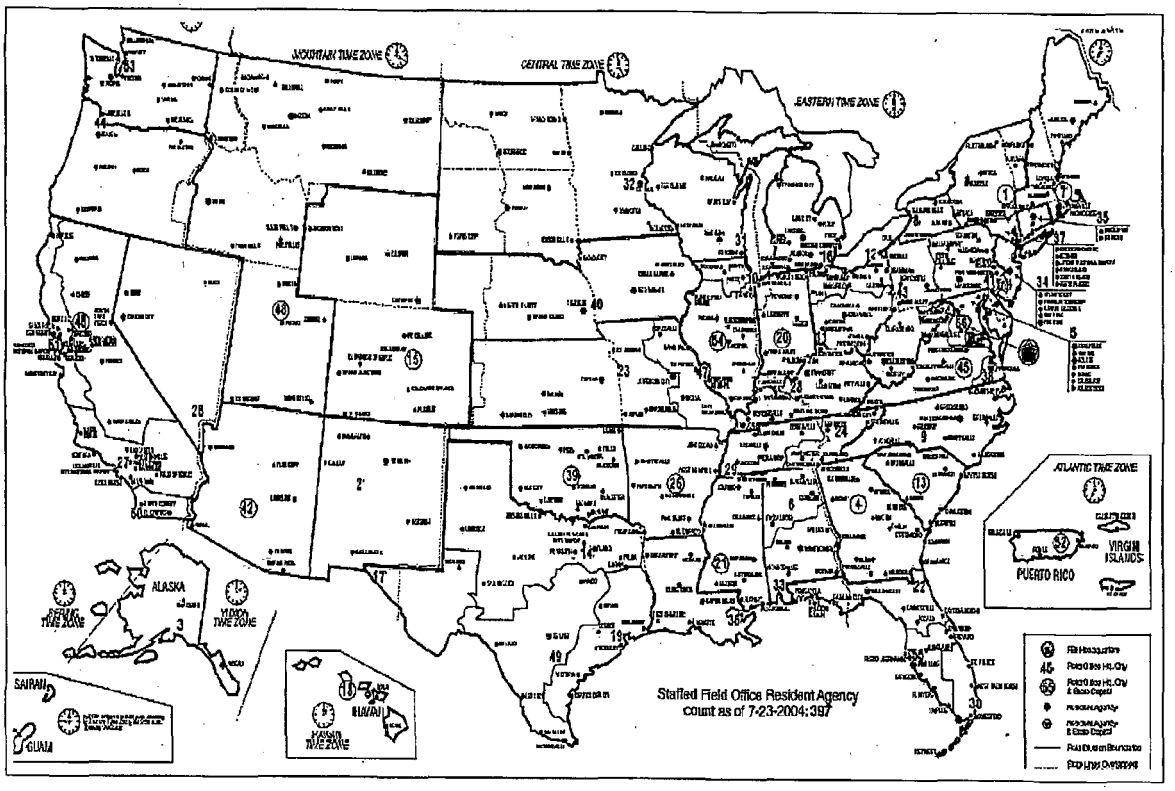
FBI/Counterterrorism/JTTF Organization

UNCLASSIFIED//FOR OFFICIAL USE ONLY

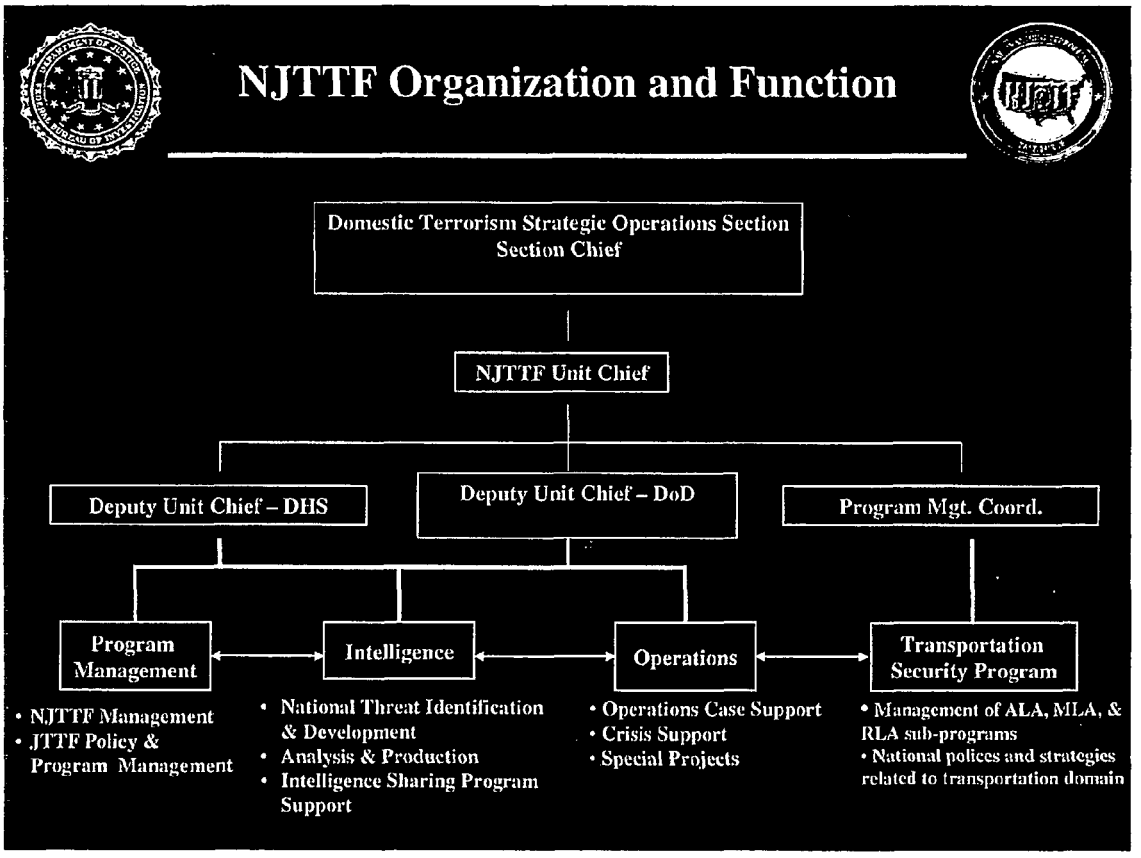
COUNTERTERRORISM DIVISION



UNCLASSIFIED//FOR OFFICIAL USE ONLY



UNCLASSIFIED//FOR OFFICIAL USE ONLY


NJTTF Organization and Function
Domestic Terrorism Strategic Operations Section
Section Chief
NJTTF Unit Chief
Deputy Unit Chief – DHS
Deputy Unit Chief – DoD
Program Mgt. Coord.
Program Management
Intelligence
Operations
Transportation Security Program
• NJTTF Management
• JTTF Policy & Program Management
• National Threat Identification & Development
• Analysis & Production
• Intelligence Sharing Program Support
• Operations Case Support
• Crisis Support
• Special Projects
• Management of ALA, MLA, & RLA sub-programs
• National polices and strategies related to transportation domain

TFO/TFA IN-PROCESSING LIST

1) Security
   a) SF-86 (Category I - Full Top Secret Background must cover 10 years)
   b) Initial FD-857 and FD-868 (retained at until Official Security Clearance comes back. Initial must be destroyed).
   c) Final Set of noted forms are sent with EC requesting Computer Access and RA Access Badges.
      i) Security Clearance Brochure
      ii) PSI
      iii) NCIC Checks
      iv) ACS Checks
      v) IA Checks
      vi) Local Involvements
      vii) NADDIS Checks
      viii) Fingerprints
   d) SCI Indoctrination (if applicable)
   e) For individuals possessing a Security Clearance from their "home" agency, they must have it passed from their agency to FBIHQ, Security Office.

2) MOU, Reimbursement Agreement, Venders Forms
   a) Send EC to NJTTF via SAHQ (Coordinator's responsibility)

3) RA Access Badge/Public Key Infrastructure (PKI) - (See Coordinator)
   a) FD-889
   b) FD-857
   c) FD-868
   d) SF-312
   e) Security Awareness
   f) PKI registration form and subscriber agreement

4) Deputation (TFO's only)
   a) USM-3R
   b) FD-739
   c) Photo
   d) Appropriate EC must be forwarded to NJTTF (Coordinator's responsibility)

5) Credentials - (Must have FD-281/FBI Hand Receipt)
   a) FD-281 is turned into FBI Property Management Unit with EC

6) Photograph
   a) One Photograph is used for both Access Badge and Credentials
   b) Contact office photographer to schedule photograph

7) Computer Access (Access EC and Security Forms)
   a) FBI Data Base Access (Access EC and Security Forms)

b) FBI Computer Security Training (InfoSec, etc)

8) Biographic Sheet (Bio-Sheet) (May be required)
   a) Obtain form from Coordinator
   b) Complete form and return 3 copies to Coordinator

9) JTTF Vehicles & Gas Cards (See Coordinator)

10) Equipment Issue (FD-281 FBI Hand Receipt) (Issued equipment varies by Division)
   a) Vehicle/Gas Card (see 9 above)
   b) Pager
   c) Vest
   d) Hand-held Radio
   e) Cell Phone
   f) Car Radio Packet
   g) Portable Police Emergency Lights
   h) Blackberry

11) Radio Frequencies/Call Signs – See JTTF Coordinator or appropriate POC

12) TFO's Chain of Command at their agency
   a) Provide Information to Coordinator

13) TURK (Time Utilization Record Keeping)
   a) Forms are maintained by Administrative Assistant
   b) Complete form weekly

14) Electronic Equipment Security Form
   a) Obtain forms from Coordinator
   b) Read and sign Acknowledgment Form
   c) Fill out Electronic Equipment Registration Form and return to Coordinator

15) Law Enforcement On-Line (LEO)
   a) Obtain form from Coordinator
   b) Complete form and obtain appropriate signature from your supervisor
   c) Return form to LEO Coordinator

16) Internet Access
   a) Obtain form from Coordinator
   b) Complete form and return to Coordinator

17) Airport/Transportation Infrastructure Access badge and Briefing (where applicable)

18) Request for military base access pass (where applicable)

19) Personnel Security Polygraph Program
   a) All personnel detailed to the FBI JTTF are required to submit to a polygraph examination prior to obtaining a security clearance.

SECURITY CLASSIFICATION GUIDE

Background: On October 31, 2008, President Bush issued Executive Order 12333, which set forth the most current procedures for dealing with classified information, including:

- Safeguarding National Security Information
- Levels of Classification
- Declassification

DEFINITIONS

Information: Any knowledge that can be communicated or documentary material that is owned by, produced by or for, or is under the control of the U.S. Government.

Classification: That process used by an Original Classification Authority to determine what information should be classified and at what level.

Classified National Security Information: Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

National Security Information: Information, which if disclosed, would cause harm to the National Security or foreign relations of the United States.

CLASSIFICATION

There are three levels of Classifications:

1. ~~CONFIDENTIAL~~: Unauthorized disclosure may cause DAMAGE to National Security.
2. ~~SECRET~~: Unauthorized disclosure may cause SERIOUS DAMAGE to National Security.
3. ~~TOP SECRET~~: Unauthorized disclosure may cause EXCEPTIONALLY GRAVE DAMAGE to National Security.

Terms such as
"For Official Use Only"
or
"Law Enforcement Sensitive"
Do not refer to
Levels of Classification

"For Official Use Only" is a caveat regarding the dissemination of intelligence information. For Official Use Only information can only be disseminated to other official US government agencies that have a need to know.

"Law Enforcement Sensitive" is another caveat regarding the dissemination of intelligence information. Law Enforcement Sensitive information can only be disseminated to other local, state or federal law enforcement agencies.

RESTRICTIVE HANDLING CAVEATS AND CONTROL MARKINGS

- **ORCON** - Originator Controlled; Dissemination and Extraction of Intelligence information is controlled by the Originator of the Information
- **NOFORN** - Not releasable to Foreign Nationals

SAFEGUARDING

Protection of Classified Information from Unauthorized Disclosure

- Access
- Marking
- Transmission
- Storage

- **CLEARANCE + NEED TO KNOW = ACCESS**
- **OVERALL DOCUMENT MARKING** - A document's overall classification is determined by the HIGHEST classification level of information contained on any page of that document.

~~SECRET~~

If a document contains more than one page, place the overall classification marking conspicuously at the top and bottom of the front cover, on all documents pages, and at the top and bottom of the outside of the back cover.

PORTION MARKINGS

Indicate classification level of each portion of the document.

- Subject
- Title
- Paragraphs
- Graphics

PORTION MARKING PART II

Indicate classification level (including caveats) in ( ) immediately preceding or following the portion to which it applies.

~~(TS) Top Secret~~
~~(S) Secret~~
~~(C) Confidential~~
(U) Unclassified

METHODS OF TRANSMISSION

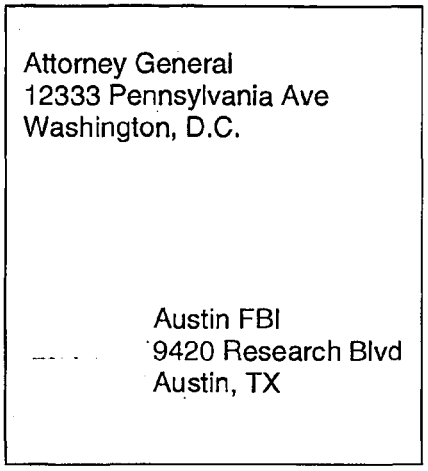
- U.S. Postal Service
- Contracted Service
- Authorized DOJ, DOD, DOS, or component courier service/system
- Cleared and designated government employee
- Authorized cryptographic system

Preparation of Material for Transmission

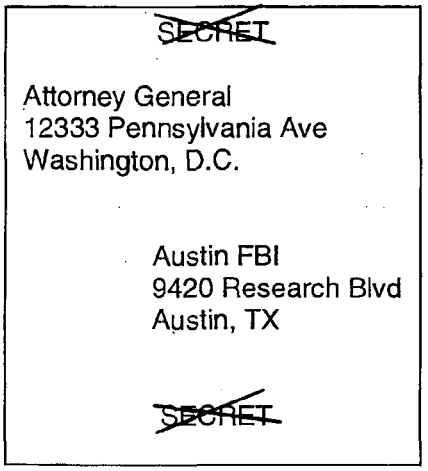
- ✓ Envelopes or containers
- ✓ When classified information is transmitted, it will be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and to ease in detecting tampering.

Addressing

- ✓ The outer envelope or container for classified material will be addressed to an official government activity or to a DOD contractor with a facility clearance and appropriate storage capability. It will show the complete return address of the sender. The outer envelope will not be addressed to an individual. Office codes or phrases such as "Attention: SA Smith may be used.
- ✓ The inner envelope or container will show the address of the receiving activity, the address of the sender and the highest classification of the contents.
- ✓ The outer envelope or single container will not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.



Outer opaque wrapping/cover



Inner opaque wrapping

Transporting

- ✓ When being hand carried outside an activity, a locked briefcase or locked bag may serve as the outer wrapper, but not when hand carried aboard a commercial airline.

Desk Reference
Intelligence Community Classification Markings

http://www.intelink.sgov.gov/sites/ssc/capco/marking_refs/Marking%20References%20Documents/CAPCO%20Implementation%20Manual_2.1_5%20January%202009.pdf (This URL is on the FBINet system.)

The Intelligence Community format for marking classified information requires a banner line and portion markings on every page, and a classification authority block on the face of each document or media. The format for banner lines and portion markings consists of eight categories (as described in gray box below). The IC format also specifies how to separate the categories and series of markings within them. The categories must be listed in the order shown in the *Authorized Classification and Control Markings Register*. Use only categories and markings required to protect the information. The banner line below* (see yellow arrow) is an example of the formatting and ordering of the most frequently used categories and required punctuation. It is not intended to represent a correct overall classification marking.

CLASSIFICATION. Conspicuously place the banner line at the top and bottom of each page in uppercase letters. A double slash separates categories. When necessary, break the line after a punctuation mark. Whether US, non-US, or JOINT, there will only be ONE classification designated (i.e. TS, S, C, R, U). Mark unclassified documents when transmitted over a classified system (banner line only) or when they contain dissemination controls such as FOUO or LES (banner line and portion markings).

DISSEMINATION CONTROLS. When using multiple markings, separate them with a single slash. List in order shown in *Markings Register*.

In the REL TO marking, always list USA first, followed by other countries' ISO 3166 trigraphs listed in alphabetical order by country name. Then list Annex A tetragraphs in alphabetical order. Separate trigraphs/tetragraphs with a comma and a space. The word "and" has been eliminated.

* EXAMPLE BANNER LINE → **TOP SECRET//HCS/COMINT-GAMMA/TK//FGI CAN GBR//ORCON/PROPIN/REL TO USA, FRA, FVEY**

SCI CONTROL SYSTEMS/SAP. Identify the SCI control systems and subsystems. Use a single slash (no space) to separate SCI control systems. SCI subsystems. Use a hyphen (no space) between the SCI control system identifier (e.g., COMINT) and the SCI subsystem (e.g. GAMMA). SI and COMINT are synonymous; may use SI or COMINT in banner, but must use SI in portion markings.

FOREIGN GOVERNMENT INFORMATION. Identify source of FGI in a US-originated document. In banner line, use FGI + trigraph country code in alphabetical order, separated by a single space; e.g.: FGI GBR. In portion markings, use trigraph + portion marking for classification level; e.g.: (//GBR S).

1. US Classification
2. Non-US Classification
3. Joint Classification
4. SCI Control System
5. Special Access Program
6. Foreign Government Information
7. Dissemination Controls
8. Non-Intelligence Community Markings

Eight Categories and Most Common Authorized Portion Markings*
THIS LIST IS NOT ALL-INCLUSIVE! Visit the URL at the top of this page for a COMPLETE list of markings.

1. US Classification
   - TOP SECRET (TS)
   - SECRET (S)
   - CONFIDENTIAL (C)
   - UNCLASSIFIED (U)
2. Non-US Classification
   Reserved for other countries and international orgs. Can be TS, S, C, U, or RESTRICTED (R) e.g. //GBR R or //NATO S
3. Joint Classification
   Used for information owned, produced by more than one country. Can be TS, S, C, U, or R e.g. //JOINT S CAN GBR USA

4. SCI Control Systems/Subsystems
   - HCS (HCS)
   - COMINT (SI)
     - -GAMMA (-G) (Requires ORCON)
     - -ECI [3-letter designator]
   - TALENT KEYHOLE (TK)

5. Special Access Program
   SPECIAL ACCESS REQUIRED-[program identifier] (SAR-BP)

6. Foreign Government Information
   Example: Canadian Secret information
   Banner line: //FGI CAN
   Portion Marking: (//CAN S). Use FGI and classification level ONLY (//FGI S) when origin country must be concealed.

7. Dissemination Controls

FOUO	(FOUO)
ORCON	(OC)
IMCON	(IMC)
NOFORN	(NF)
PROPIN	(PR)
Authorized for Release to...	(REL TO)
RELIDO *(new marking)*	(RELIDO)
DEA Sensitive	(DSEN)
FISA	(FISA)
Law Enforcement Sensitive	(LES)

(NOTE: In classified documents, LES is not included in the banner line. See http://www.intelink.sgov.gov/sites/ssc/capco/marking_refs/Marking%20References%20Documents/LES%20Interim%20IC%20Marking%20Guidance.doc for IC Guidance.)

8. Non-Intelligence Community Markings
   - Special Category (SC)
   - Sensitive Information (SINFO)
   - Limited Distribution (DS)
   - Exclusive Distribution (XD)
   - No Distribution (ND)
   - Sensitive But Unclassified (SBU)
   - SBU-NOFORN

* Refer to the *Authorized Classification and Control Markings Register* for a complete listing and authorized order of markings. Visit *http://www.intelink.sgov.gov/sites/ssc/capco/marking_refs/default.aspx* for the Markings Register and Implementation Manual.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI/SecD/SPCAU Updated Jul 2009/hma

SECURITY AWARENESS BRIEFING FOR FBI EMPLOYEES AND TASK FORCE OFFICERS

All FBI employees are expected to abide by the standards of conduct set forth in Title 5, CFR, Section 2635, as supplemented by DOJ regulations, and by the rules and regulations of the FBI pursuant to authorization set forth in Title 28, CFR, Section 0.137.

PERSONNEL SECURITY

1) Must uphold values of reliability, trustworthiness, honesty, and integrity.
2) Must be entirely frank and cooperative in answering inquiries of an administrative nature.
3) Must not falsify information and/or documents for purposes of fraud or personal gain.
4) Must not engage in illegal activities, criminal conduct, dishonest conduct, or insubordination.
5) Must report to the FBI any occurrence or activity which might reflect adversely on the FBI or bring discredit to the Bureau.
6) You are proscribed from managing any business or sales activity inside FBI space that you might have in connection with any other employment(s) in which you might be involved.
7) It is improper to engage in any illegal gambling activities. You should not participate in lotteries, pools, betting, bookmaking, etc., while in official duty status or government property occupied by the Bureau.
8) You are accountable for your on/off duty alcohol-related misconduct whether or not you are specifically charged with an alcohol-related offense. Never cause yourself to be unfit for duty due to excessive alcohol consumption. A first DUI infraction, whether established by a conviction in court or as the result of an administrative inquiry, will cause you to be suspended from duty without pay for a period of not less than 30 calendar days. If aggravating circumstances exist, you may be terminated from employment.
9) You may not solicit or collect contributions for any purpose while in Bureau space without prior FBI approval.
10) Gifts, discounts, benefits, reduced memberships, etc., are prohibited if it was offered as a result of your employment. Such gratuities might be acceptable if they are offered to all FBI employees, not just you. These gratuities may not be accepted if offered by a "prohibited source" or if a conflict of interest exists.
11) You may give employment recommendations or act as a character reference for Bureau personnel so long as your response is not based on FBI files or on any information or data that you acquired by virtue of your federal employment. Do not use Bureau stationary, letters with the FBI seal, or your official title or position in your response. Your response is your personal opinion and not the opinion of the FBI.

12) You are expected to maintain a satisfactory credit reputation and promptly pay all of your debts.
13) It is incumbent upon you to stay current on any court-ordered obligations, such as child support, alimony, etc.

14) The following must be reported to your Division Security Officer:
    a) Requests to engage in outside employment. You may not accept any other employment without prior SAC/FBIHQ approval.
    b) Requests to have a roommate (a non-family member residing with you for more than 30 days)
    c) Marriages: 60 days prior to the marriage date;
    d) All types of arrests and civil litigations (i.e., divorce, separation, annulment, etc.);
    e) Aggravated traffic violations;
    f) If you become a subject/suspect in a criminal matter;
    g) Financial problems:
        i) Filing for bankruptcy
        ii) Accounts placed for collection
        iii) Property repossessed
        iv) Liens placed against you, including wage garnishments
        v) Civil judgments
        vi) Foreclosures
    h) Foreign travel: 30 days prior to your travel (this includes official/unofficial foreign travel and any short excursions or day trips to other countries);
    i) All contact with foreign nationals residing abroad or in the United States;
    j) Gifts received from a foreign government.
15) An EAP counselor is available for consultation and guidance should you experience emotional stress, personal problems, etc.
16) If you have been issued a Government Credit Card, it is for official use only. Personal use to obtain goods, services, cash, etc., and nonpayment for undisputed balances may be cause for suspension and/or revocation of your security clearance.
17) ALL FBI-owned, rented, or leased vehicles are to be used for official business only.
18) No family members are permitted in any vehicle utilized by the Bureau without SAC approval.
19) The loss or destruction of certain Bureau property has security ramifications and must be vigilantly avoided. Any loss of Bureau property must be immediately reported to your supervisor and to the Division Security Officer. Any loss of personal property within Bureau space should also be reported to the SO.

FACILITY SECURITY

1) Do not permit your Security Access Control System (SACS) badge to be photographed or photocopied at any time.
2) Safeguard your SACS badge at all times and do not leave it unattended.

3) Immediately notify the Division Security Officer if your SACS badge is lost, stolen, or misplaced.
4) Your SACS badge is to be visibly worn at all times while in FBI space; do not openly display it in public areas.
5) Employees have the right, and responsibility, to challenge (ID) anyone in FBI space who is not properly identified.
6) Do not share your SACS badge or access code number with any other person (not even another FBI employee).
7) Door Code: Do not share it with anyone. If you do, your door code will be deleted, and you will not have electronic access to FBI space until after you have met with your Division Security Officer.
8) Become familiar with the various types of badges:
   a)
   b)
   c)
   d)
9) When entering FBI space, take notice of those around you as a precautionary method in preventing unauthorized persons from entering FBI space. If you do not know an individual attempting to enter FBI space, ID them. Make sure the door closes behind you, thus preventing someone from gaining unauthorized access to FBI space. b7E
10) Visitors must be escorted at all times while in Bureau space and wear an appropriate
11) The last employee to leave a work area at the close-of-business must ensure the area is secure and classified material is appropriately stored.

INFORMATION SECURITY/COMPUTERS

1) All FBI employees have a ~~Top Secret~~ security clearance; but not all FBI employees have a need-to-know what you are working on. An appropriately cleared individual may have a legitimate need-to-know if they require information you possess in order to perform their official duties. You have the authority and are empowered to grant or deny others access to information you possess. It is your responsibility to confirm the requestor's official Bureau need to obtain information about your case in order to accomplish his/her job. Inquire about the other person's request for information. If he/she cannot convince you of the official Bureau need for access, you should deny the request. Curiosity is not a valid justification for any attempt to gain access to Bureau information or space. Do not disclose information to other persons who do not have a need-to-know (this includes even your closest relatives and friends).
2)
   A ~~Top Secret~~ security clearance does not automatically grant you access to all FBI office space and to all FBI information. b7E

3) The security of FBI space and information, the nature of FBI work, and the security of FBI personnel and their Bureau-issued property are ~~confidential~~ in nature and should not be discussed with individuals who do not have a need-to-know.
4) Employees should not needlessly identify themselves as FBI employees, particularly in restaurants and other public spaces where they might easily be within earshot of representatives of Foreign Intelligence Services or other criminal organizations. Neither should employees discuss Bureau work at luncheons, in car pools, or in other areas outside the working space, even with a social group consisting solely of Bureau employees.
5) Do not allow unauthorized persons to use Bureau computers.
6) Do not leave your work area if you are still logged onto the computer. Exit all programs (especially FBINET) before you leave your computer unattended.
7) Computer password: do not leave it on a post-it where people can see it, i.e., on the computer, under your desk, etc. Do not share it with others.
8) All FBI information is categorized as Classified or Unclassified but Sensitive (the latter being equivalent to Law Enforcement Sensitive).
9) From 1985 to 1999, seventy-five federal employees were convicted of espionage. Only two of the 75 employees sought employment with the sole intent to commit espionage. Also, approximately 80% of espionage is committed by insiders. In almost every case, these insiders gained access to information not pertinent to their jobs by circumventing the need-to-know principle. They were able to do so because their co-workers failed to properly restrict access to classified and/or law enforcement sensitive information under their control.
10) Working copies of official Bureau documents are for official business and not for personal use.
11) Unsolicited telephone inquiries for FBI information should not be disclosed if the identity of the caller is unknown and/or if the caller does not have a need-to-know. Classified information cannot be discussed over non-secure telephone lines.
12) Official, unclassified Bureau trash must be disposed of via the use of white-rimmed wastebaskets. These wastebaskets are to be emptied each day at the close-of-business.
13) Whenever Bureau mail of any type is carried on elevators, in corridors, or in other public spaces, the material should be covered.
14) Bureau work should not be taken into restrooms or lounges at any time.
15) You are not allowed to take home investigative files or serials.

THREATS TO NATIONAL SECURITY

1) The possibility exists that you could become a target of recruitment from various groups/entities who seek information from the FBI. Why are you a target?
   a) Your employment with the FBI;
   b) You are perceived as having access to an intelligence agency; and
   c) You have access to a law enforcement agency.

2) Who may target you?
   a) Organized drug rings
   b) Gangs
   c) Mafia organizations
   d) Individual drug dealers
   e) White collar criminals
   f) International and domestic terrorist groups
   g) Radical militant groups
   h) Foreign intelligence services
3) How could you be targeted?
   a) Recruitment: Your cooperation can be actively solicited by any of the aforementioned groups;
   b) Volunteer: Your willingness to provide information, of your own volition, motivated by factors such as greed, discontentment, dissatisfaction, revenge, etc.
   c) Coercion: Using extortion tactics to exert pressure on you as a means to force you to cooperate;
   d) Compromise: Attempts to put you in a situation that could jeopardize your affiliation with the FBI if you do not cooperate with them, such as sex, drugs, prostitution, criminal acts, etc.
4) You have an affirmative obligation to notify the Bureau in writing if you become a target, or suspect that you may have become a target.
5) If you observe something contrary to good security, contact the Division Security Officer.
6) If you are experiencing financial difficulty, emotional stress, personal problems, etc., contact your EAP Counselor and/or seek professional counseling.
7) If you have any questions, call the Division Security Officer

TELEPHONE AND FACSIMILE MACHINE

1) Telephones are not considered secure. Any classified conversation should be conducted on a STU or STE telephone.
2) Facsimile machines are not considered secure and should not be used for classified information. Classified documents should be faxed on secure fax machines and those clearly marked for the transmittal of classified information. SCI information may only be sent from and received in an approved SCIF by an authorized person maintaining the appropriate accesses. SCIF locations vary, but the presence of FBI personnel does not necessarily indicate the presence of a SCIF.

SECURITY INCIDENT PROGRAM

1) The goal of the Security Incident Program (SIP) is to reduce the number of security incidents on the part of FBI personnel and associates (JTTF, contractor, vendor, detailee). This can largely be accomplished through education of the FBI population, which will lead to committed vigilance to protect FBI and IC equities.

2) A security incident is a failure to safeguard FBI material in accordance with FBI policies and other IC directives and is categorized as a violation or an infraction. **A security violation is any incident that results in the actual loss, compromise, or suspected compromise of classified national security information or unclassified information.** For example, if an employee transmits a classified document over an unclassified facsimile machine, the incident would be determined to be a security violation, due to the real possibility for electronic interception and transcription of the classified document. **A security infraction is any other incident that is not in the best interest of security and that does not involve the loss, compromise, or suspected compromise of classified national security information.** For example, at the end of a workday, an employee leaves a security container unlocked and unattended, containing classified information, in an area approved for storage of classified information. No unauthorized entry took place. This incident would be determined to be a security infraction because Bureau policy requires that classified material be secured properly after hours, even though no actual compromise occurred in this case.
3) When a security incident occurs, swift and efficient attention must be afforded to ensure the minimization of any possible damage through notification to the appropriate authorities. Security incidents should be reported immediately utilizing the SIP form located on the Security Division Website. Instructions are included with the form, which is prompting, based on the information provided by the reporting individual.

PROPER HANDLING OF FEDERAL TAXPAYER INFORMATION (FTI)

1) Internal Revenue Code (IRC) prescribes felony penalties for Federal employees who make illegal disclosures of Federal Tax returns and return information. IRC makes unauthorized inspection of FTI by a Federal employee a misdemeanor offense, plus discharge from federal employment. IRC prescribes civil damages for unauthorized inspection or disclosure of FTI. The FBI is authorized to receive FTI but must have adequate programs in place to protect the information received.

2) Oversight of the safeguarding of FTI is delegated to the Security Compliance Unit, Security Operations Section, Security Division, and FBIHQ. Each field office must establish and maintain uniform safeguard standards consistent with IRS guidelines. A Taxpayer's Information field has been established in ACS, therefore, all FTI entered should be appropriately marked.
3) FBI is required to establish a permanent system of standardized records of requests made, by or to them, for disclosure of FTI, including requests among employees, as well as from outside agencies. Authorized employees must be responsible for securing magnetic tapes/cartridges containing FTI before, during and after processing.
4) FBI is required to restrict access to FTI only to persons whose duties or responsibilities require access on a need-to-know basis. FTI should be clearly

marked "Federal Taxpayer Information." It is recommended that FTI be kept separate from other information to avoid inadvertent disclosure. In cases where the information may not be physically separated, the file should be clearly labeled to indicate that FTI is contained in the file.

5) FTI will be furnished by the IRS to state tax agencies only for administration purposes. Further disclosure by authorized receiving state agency is not permitted.
6) Granting an employee access to FTI should be preceded by certifying each employee understands the FBI's policy and procedures for safeguarding FTI.
7) FTI, including any copies made, must be returned to the IRS or render the information "un-Disclosable." If information is returned to IRS, use a receipt process and maintain Confidentiality of information. Otherwise, FTI should be destroyed by burning, mulching, pulping, shredding or disintegrating.

SECURITY AWARENESS CERTIFICATION

I acknowledge that I have been afforded a Security Awareness Briefing regarding my responsibilities as an employee of the FBI. My signature below asserts that I fully comprehend my security related duties/responsibilities and affirms my commitment to the FBI's security policies, regulations, and procedures

(Do not sign. This is an example only)

(Individual Briefed / Print Name) (Signature) (Date)

CRIMINALIZING TERRORISM[1]

The United States Constitution recognizes the inviolable right to free expression and free association, and the right to be free from deprivations of liberty or property without "due process of law." As interpreted by American courts, persons in the United States cannot be prosecuted for their thoughts alone, nor can the United States criminalize conduct protected by the First Amendment. As a result, our criminal jurisprudence stresses definable acts, rather than thoughts or speech unattached to particular conduct.

The structure of terrorism crimes prosecuted in the United States follows this tradition. There is no crime of "being a terrorist" or "thinking terrorist thoughts." While the United States Code defines the "federal crime of terrorism" (Title 18, United States Code, Section 2332b (g)(5)), as an offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and it then simply lists all the terrorism-related crimes for ease of reference. Persons cannot be convicted of the "federal crime of terrorism," because there is no such crime. Title 18 does define "international terrorism" and "domestic terrorism" in section 2331. Both pertain to activities that involve acts that are dangerous to human life, that are a violation of federal or state criminal law, that appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping. The major distinction is that international terrorism occurs primarily outside

[1]Counterterrorism Enforcement: A Lawyer's Guide by Jeff Breinholt, Office of Legal Education, U. S. Department of Justice, May 2004.

the territorial jurisdiction of the United States and domestic terrorism occurs primarily within the United States.

Terrorism crimes have developed in the same manner as other law enforcement areas. Policymakers determine what negative results should be prevented, and then craft criminal laws that take into account how such results are generally achieved. On occasion, acts that are criminalized are not ones that should necessarily be discouraged, if committed by persons not otherwise involved in the offensive conduct sought to be prevented. In such cases, laws are crafted to criminalize such conduct only when committed in particular circumstances. A good example is title 31 U.S.C. §5324, Structuring Currency Transactions. Congress crafted this statute to target persons who make large sums of cash by illegal means; drug dealers, fences, etc. The law prohibits conduct that is not inherently offensive (making several large cash deposits in a single day) in those circumstances that separate the innocent from the guilty. A legitimate cash businessman has no problem filing the required report while the criminal attempts to avoid the report to keep from coming to the attention of authorities.

Some of the various crimes that may be utilized in investigating "terrorism" are listed below. In line with our legal tradition, these crimes are based on the recognition of how terrorists behave, rather than what they believe and who they are as the emphasis is on acts rather than status or beliefs. An asterisk (*) next to the title of the offense denotes that it is listed as a "Federal crime of terrorism" within 18 U.S.C. § 2332b (g) (5). These offenses apply to "international terrorism" or "domestic terrorism" cases or to both. Not all of the following statutes come within the jurisdiction of the FBI but may be applicable to other agencies associated with the JTTF, nor is the list inclusive.

STATUTES

Title 8

§ 1324	Alien smuggling
§ 1325	Illegal entry by an alien
§ 1326	Unlawful reentry of a deported alien
§ 1328	Importation of aliens for immoral purposes

Title 18

§ 32	Destruction of aircraft or aircraft facilities*
§ 37	Violence at international airports*
§ 43	Animal enterprise terrorism
§ 81	Arson within special maritime and territorial jurisdiction*
§ 112	Assaults of foreign officials, official guests, and internationally protected persons
§ 113	Assaults within special maritime and territorial jurisdiction
§ 175	Prohibitions with respect to biological weapons*
§ 175b	Possession by restricted persons*
§ 229	Prohibited activities (relating to chemical weapons)*
§ 231	Civil disorders
§ 232	Definitions
§ 351	Congressional, Cabinet, and Supreme Court assassination, kidnapping and assault*
§ 373	Solicitation to a crime of violence
§ 831	Prohibited transactions involving nuclear materials*
§ 842	Unlawful acts (relating to explosives)*

§ 844	Penalties (regarding to arson and bombing)*
§ 878	Threats and extortion against foreign officials, official guests, or internationally protected persons
§ 922	Unlawful possession of a firearm
§ 930	Possession of firearms and dangerous weapons in federal facilities*
§ 951 et seq	Neutrality violations
§ 956	Conspiracy to murder, kidnap, or maim persons abroad*
§ 960	Expedition against a friendly nation
§ 1028A	Aggravated identity theft
§ 1030	Fraud and related activity in connection with computers*
§ 1038	False information and hoaxes
§ 1114	Protection of officers and employees of the United States*
§ 1116	Murder or manslaughter of foreign officials, official guests, or internationally protected persons*
§ 1201	Kidnapping of foreign officials, official guests, or internationally protected persons
§ 1203	Hostage taking*
§ 1362	Communication lines, stations or systems*
§ 1363	Buildings or property within special maritime and territorial jurisdiction*
§ 1365	Tampering with consumer products
§ 1366	Destruction of an energy facility*
§ 1751	Presidential and Presidential staff assassination, kidnapping, and assault*
§ 1956	Money laundering
§ 1957	Unlawful monetary transaction
§ 1960	Operating an unlicensed money transmitting business

§ 1958	Murder for hire
§ 1992	Wrecking trains*
§ 1993	Terrorist attacks and other acts of violence against mass transportation systems*
§ 2101	Riots
§ 2102	Definitions
§ 2155	Destruction of national-defense materials, national-defense premises, or national-defense utilities*
§ 2280	Violence against maritime navigation*
§ 2281	Violence against maritime fixed platforms*
§ 2331	Terrorism definitions
§ 2332	Terrorism criminal penalties*
§ 2332a	Use of certain weapons of mass destruction*
§ 2332b	Acts of terrorism transcending national boundaries*
§ 2332d	Financial transactions
§ 2332f	Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities*
§ 2339	Harboring terrorists*
§ 2339A	Providing material support to terrorists*
§ 2339B	Material support to terrorist organization*
§ 2339C	Relating to financing terrorism*
§ 2340A	Torture*
§ 2384	Seditious conspiracy
§ 2381	Treason

Title 31

§ 5324(a) (3) Structuring transaction to evade reporting requirements

Title 42

§ 2284 Sabotage of nuclear facilities or fuel*

Title 49

§ 46502 Aircraft piracy*

§ 46504 Interference with flight crew members and attendants*

§ 46505 Carrying a weapon or explosive on an aircraft*

§ 46506 Application of certain criminal laws to acts on aircraft*

§ 46507 False information and threats

§ 60123 Destruction of interstate gas or hazardous liquid pipeline facility*

Title 50

§ 1701 Illegal transactions with prohibited groups or individuals

INVESTIGATIVE GUIDELINES

The United States Attorney General has established Guidelines to have a consistent policy in the specified matters and to enable agents to perform their duties with greater certainty, confidence and effectiveness, and assure the American public that the FBI is acting properly under the law. Two separate and distinct Guidelines have been established. One, "The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations" govern the circumstances under which general criminal and criminal intelligence investigations are conducted by the FBI. The investigations pursuant to these Guidelines are applicable to Domestic Terrorism

(DT) investigations using the "Terrorism Enterprise Investigations (TEI)" section and are worked by the JTTF [redacted] b7E

In their general structure, both Guidelines provide graduated levels of investigative activity, allowing the FBI the necessary flexibility to act well in advance of the commission of planned terrorist acts or other federal crimes. The three levels of investigative activity are: (1) Threat Assessment (TA), the prompt and extremely limited checking of initial leads, (2) Preliminary Investigation (PI), and (3) Full Field Investigation (FFI). The conduct of investigations authorized under the Guidelines may present choices between the use of information collection methods that are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. As Executive Order 12333 § 2.4 provides, "the least intrusive collection techniques feasible" are to be used in such situations. It is recognized, however, that the choice of techniques is a matter of judgment. The FBI must comply with all requirements for use of a technique set by statute, Department regulations and policies, and Attorney General Guidelines. The following general descriptions of investigations apply to both DT and IT investigations. [redacted] The applicable b7E guideline provides specific authority for the investigations and should be reviewed and

relied upon. These general descriptions are provided to assist a new task force member upon initial assignment to the JTTF.

Assessments:

The lowest level of investigative activity is the "prompt and extremely limited checking out of initial leads," which should be undertaken whenever information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted. This limited activity should be conducted with an eye toward promptly determining whether further investigation (either a Preliminary Investigation or Full Field Investigation) should be conducted.

Preliminary Investigation (PI):

The next level of investigation is the Preliminary Investigation. A PI is short of a Full Field Investigation and allows the government to respond in a measured way to ambiguous or incomplete information, with as little intrusion as the needs of the situation permit. Such inquiries are carried out to obtain the information necessary to make an informed judgment as to whether a Full Field Investigation is warranted. A PI is not a required step. When facts or circumstances reasonably indicating criminal activity are already available, a Full Field Investigation can be immediately opened. Where a PI fails to disclose sufficient information to justify a Full Field Investigation, the FBI shall terminate the investigation and make a record of the closing.

All lawful investigative techniques may be used in a PI **except** mail openings, non-consensual electronic surveillance or any other investigative technique covered in Title 18, United States Code, §§2510-2552. (See the current DIOG, and "*Use and Approvals for Investigative Techniques*" in Tab 6).

Full Field Investigation (FFI):

There are several types of Full Field Investigations conducted by the FBI.

[redacted] b7E

[redacted] They, of course will be available once the TFO has his clearance. For DT investigations two, general crimes investigations (FBI Classification 266) and Terrorism Enterprise Investigations (FBI Classification 100), will be discussed. The choice of the type of investigation depends on the information and investigative focus. A general crimes investigation may be initiated where facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed. Preventing future criminal activity, as well as solving and prosecuting crimes that have already occurred, is an explicitly authorized objective of general crimes investigations. The "reasonable indication" threshold for undertaking such an investigation is substantially lower than probable cause.

A TEI is the second type of FFI in a DT investigation and is a criminal intelligence investigation. The focus of criminal intelligence investigations is the group or enterprise, rather than just individual participants and specific acts. The immediate purpose of such an investigation is to obtain information concerning the nature and structure of the enterprise—including information relating to the group's membership, finances, geographical dimensions, past and future activities, and goals—with a view toward detecting, preventing, and prosecuting the enterprise's criminal activities. Criminal intelligence investigations, usually of a long-term nature, may provide vital intelligence to help prevent terrorist acts. The threshold is the same as for general crimes, "reasonable indication".

All lawful investigative techniques may be used in a FFI including, among others, use of confidential informants, undercover activities and operations, interviews and pretext interviews of the subject and others, mail covers, physical, photographic, and video surveillance, polygraph examination, grand jury subpoenas, nonconsensual electronic surveillance, pen registers and trap and trace devices, accessing stored wire and electronic communications and transactional records, consensual electronic monitoring, and searches and seizures. All requirements for the use of such methods under the Constitution, applicable statutes, and Department regulations or polices must, of course, be observed. (See "*Use and Approvals for Investigative Techniques*" in Tab 6).

CONCLUSION

The United States counterterrorism enforcement mission was permanently altered on September 11, 2001. One of the most significant changes was the role of the federal prosecutor and the enforcement of federal laws relating to terrorism. Immediately after the 9/11 attacks, the Attorney General announced that the primary task of the Department of Justice would be preventing future terrorist attacks before they occur.

This was not necessarily a new concept, as federal prosecutors have long been involved in the early stages of criminal investigations. The true significance of this position stems from the urgency of the mission, the clarity of the mandate, and other systemic changes that followed the Attorney General's announcement. The new priority is on prevention of attacks rather than investigation and prosecution after an attack. Criminal prosecution is just one of the many tools available to realize the mission of identifying, preventing, and deterring acts of terrorism within the United States.

REQUIRED DOCUMENTATION

- Opening an Assessment
  - ✓ Open a Guardian Assessment

- Closing an Assessment
  - ✓ Closing EC

- Converting an Assessment to a Preliminary Investigation or Full Field Investigation
  - ✓ (same as Opening Preliminary Investigation or Full Field Investigation above)

- Opening a Preliminary Investigation
  - ✓ EC (Includes Opening information, Notification of Initiation and VGTOF entry)
  - ✓ Opening LHM (enclosed as an attachment)
  - ✓ VGTOF Form/FD-930

- Closing a Preliminary Investigation
  - ✓ Closing EC *Must include justification for closing case
  - ✓ Closing LHM (enclosed as an attachment)
  - ✓ VGTOF Removal Form (FD-930)
  - ✓ Notification to Department of Justice (FD-320)
    *Only if case is opened by United States Attorney's Office

- Extending a Preliminary Investigation
  - ✓ Extension EC

- Converting a Preliminary Investigation to a Full Field Investigation
  - ✓ Conversion EC
  - ✓ LHM

- Opening a Full Field Investigation
  - ✓ EC (Includes Opening information, Notification of Initiation and VGTOF entry)
  - ✓ Opening LHM (enclosed as an attachment)
  - ✓ VGTOF Form/FD-930

- Closing a Full Field Investigation
  - ✓ Closing EC *Must include justification for closing case
  - ✓ Closing LHM (enclosed as an attachment)
  - ✓ VGTOF Removal Form (FD-930)
  - ✓ Notification to Department of Justice (FD-320)
    *Only if case is opened by United States Attorney's Office

- Extending a Full Field Investigation
  - ✓ Extension EC

- Annual Summary for a Full Field Investigation
  - ✓ Annual Summary EC
  - ✓ Annual Summary LHM

- Issuing a Grand Jury Subpoena
  - ✓ Subpoena Request Form
  - ✓ FD-302

- Reporting Grand Jury Subpoena Return
  - ✓ FD-302

- Issuing a National Security Letter
  - ✓ NSL (LHM)
  - ✓ NSL EC (Created within FISAMS)
  - ✓ FD-542

[redacted] b7E

- Serving National Security Letter Return
  - ✓ FD-542 (Serving NSL)

- Requesting Surveillance by SSG
  - ✓ Surveillance Request Form
  - ✓ FD-542 (Requesting Surveillance)

- Reporting Surveillance Conducted by SSG
  - ✓ FD-542 (Surveillance Conducted)

- Reporting Surveillance Conducted by JTTF
  - ✓ FD-302 or Surveillance Log

- Request Training
  - ✓ FD-878
  - ✓ Training Request Form (TRF)

- Reporting an Interview
  - ✓ FD-302

- Reporting a Trash Cover
  - ✓ FD-302
  - ✓ FD-542 (to document analysis of and claim statistical accomplishment)

- Reporting a Collision
  - ✓ Collision EC
  - ✓ SF-91
  - ✓ ST-3 (Completed by Police Officer on scene)
  - ✓ Police Report (Completed by Police Officer on scene)
  - ✓ An FBI Agent must respond to scene as he/she will need to complete EC/302.
- Submitting General Evidence
  - ✓ FD-302
  - ✓ FD-597 (Evidence Log)
  - ✓ FD-192 (Evidence Submission Form)
  - ✓ Chain of Custody
- Submitting Film for Processing
  - ✓ FD-523 (AIRTEL)
  - ✓ (See contact list or JTTF Coordinator for applicable contact)
- Submitting Electronic Evidence to be Analyzed
  - ✓ FD-302 (if not already documented on evidence/surveillance logs, etc)
  - ✓ FD-597 (Evidence Log)
  - ✓ FD-192 (Evidence Submission Form)
  - ✓ Chain of Custody
  - ✓ EC to the Computer Analysis Response Team Requesting Analysis
- Submitting Toll Records to be entered into Telephone Apps.
  - ✓ Enclose in FD-340 (1A) and send to (See contact list or JTTF Coordinator for applicable contact)

Investigative Reports

EC (Electronic Communication):

The purpose of the Electronic Communication (EC) is to communicate information within the FBI.

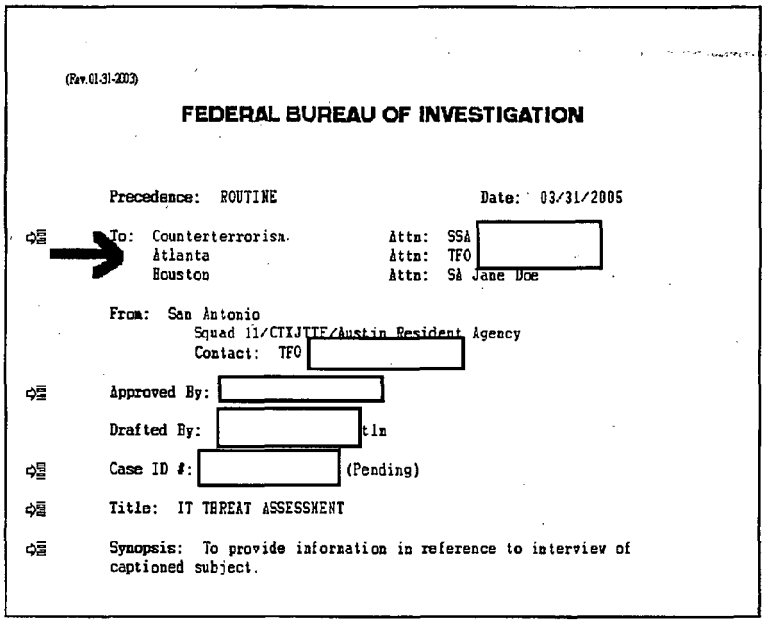
EC applications: (examples)

- Open and close cases
- Document results of a lead
- To report the status of your investigation
- Document investigative activity
- To request investigative assistance (SSG, SOG, etc...).
- To request action to be taken
- Sending information to your file

****_Can not_** claim a statistical Accomplishment**

When an EC is communicating information outside of the originating division, two components are necessary. First, your EC must contain a "*TO:*" line, indicating the division(s) receiving the EC. It is important to remember that if more than one division is listed, they must appear in alphabetical order (with Headquarters divisions listed first). **see Example 1*

Example 1



(Rev.01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 03/31/2005

To: Counterterrorism Attn: SSA
Atlanta Attn: TFO
Houston Attn: SA Jane Doe

From: San Antonio
Squad 11/CTXJTTF/Austin Resident Agency
Contact: TFO

Approved By:

Drafted By: tln

Case ID #: (Pending)

Title: IT THREAT ASSESSMENT

Synopsis: To provide information in reference to interview of captioned subject.

b6
b7C
b7E

The second requirement is a "*Lead*" section. Setting a *Lead* is a function of the EC macro and if selected, the *Lead* will automatically be placed at the end of your EC. It is important to remember that if more than one division is receiving the EC, a separate *lead* must be set for each division, and they also must appear in alphabetical order (with Headquarters divisions listed first). **see Example 2*

**NOTE: The "To:" section must correspond with the "Lead" section. That is to say that for every Division listed as a receiving division, a corresponding Lead must be set for that division.*

Following are the three approved *Lead* types:

1) "**Action Required**" - This type of lead will be used if the sending office requires the receiving office to do some action (interview victim, locate person, etc.).

2) "**Discretionary Action**" - This type of lead will be used if the sending office has some information that may be of importance to the receiving office. It may or may not require action by the recipient and the recipient will decide what, if any,

action to take. For example: Tampa receives some information regarding a crime that allegedly happened in San Francisco. Tampa forwards the information to San Francisco to take any action deemed appropriate.

3) "**Information Only**" - This type of lead will be used for information only and no specific action is required or necessary (administrative type matters, change in leave policy, etc.).

Example 2

b7E

To: Counterterrorism From: San Antonio
Re: [redacted] 03/31/2005

LEAD(s):

Set Lead 1: (Info)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2: (Discretionary)

ATLANTA

AT ATLANTA, GA

For whatever action deemed necessary.

Set Lead 3: (Action)

HOUSTON

AT HOUSTON, TX

Locate and interview Joe Terrorist, residing at 123 Main Street, Houston, TX; and report results of interview to Austin.

♦♦

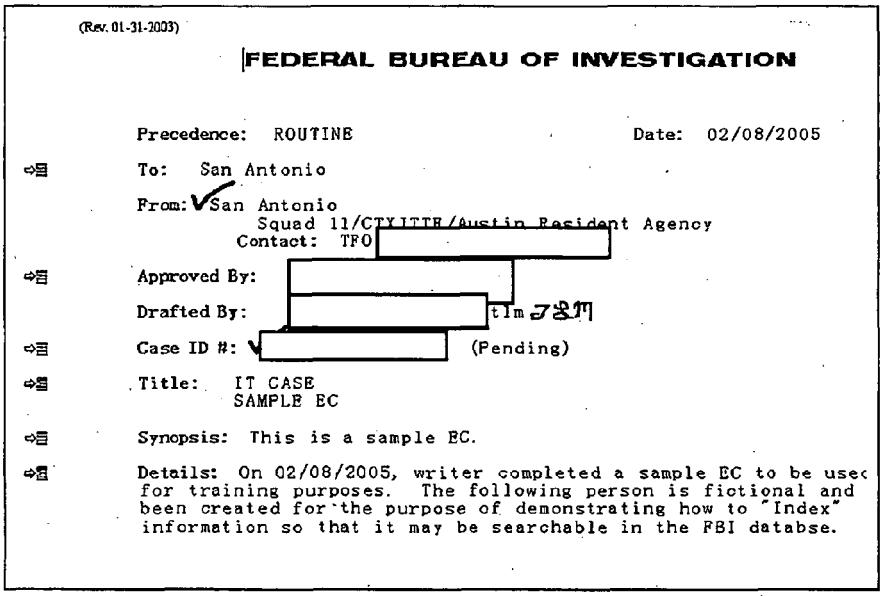
EC Copy Count: 2 (*unless one of the following: Attachments, Enclosures or covering a Lead outside of our Division.)

First copy (Original) **see Example 3*

- ✓ **Red Ink** Check mark by the "From: *Your Division*"
- ✓ **Red Ink** Check mark by the "Case ID:"
- ✓ Initial in **Black Ink** by your name next to "Drafted by:"

The **Typed initials next to your name indicate ***who actually typed*** the document, in some cases this may be different from the person who drafted it**

Example 3



(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 02/08/2005

To: San Antonio

From: San Antonio
Squad 11/CTY ITTF/Austin Resident Agency
Contact: TFO [redacted]

Approved By: [redacted]

Drafted By: [redacted] tlm 7821

Case ID #: [redacted] (Pending)

Title: IT CASE
SAMPLE EC

Synopsis: This is a sample EC.

Details: On 02/08/2005, writer completed a sample EC to be usec for training purposes. The following person is fictional and been created for the purpose of demonstrating how to "Index" information so that it may be searchable in the FBI databse.

b6
b7C
b7E

FD-542 (Statistical Accomplishment):

The purpose of the FD-542 is to communicate information within the FBI **and** claim a statistical accomplishment. **An FD-542 can be substituted for an EC in situations where you are communicating information **and** claiming a statistical accomplishment at the same time**

IMPORTANT

Your classification should be the only Case ID listed on the FD-542. If a non-valid classification (for example, administrative or criminal classification) is listed in addition to the valid classification, this would prevent the FD-542 from being uploaded.

FD-542 applications: (examples)

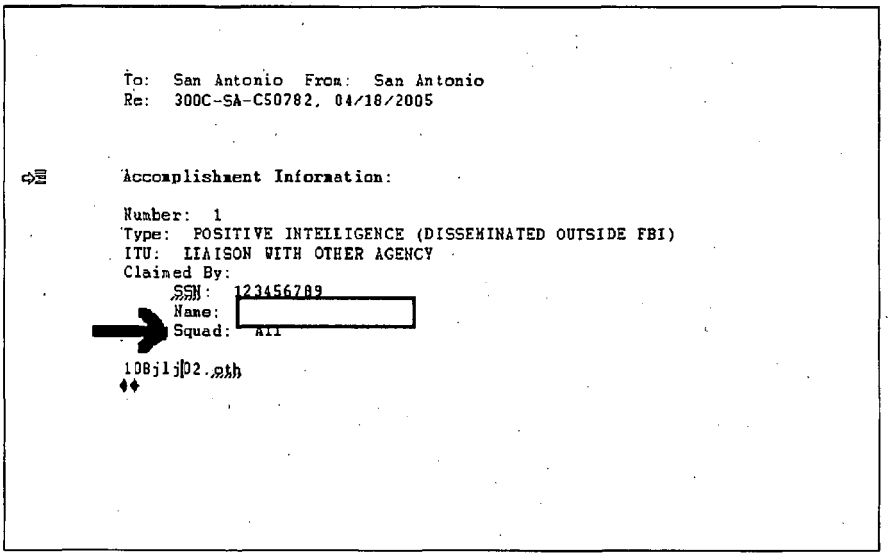
- Dissemination of information
- Participating in Command Post/Major Case/Special Event
- Participating as a Member of a WMD Working Group/Task Force
- Participation in WMD exercise
- WMD Assistance Provided to State/Local/Federal Agency
- Request Surveillance (SSG only)

- Conducting Surveillance (SSG only)
- Creating/Issuing a National Security Letter
- Serving a National Security Letter

The "*Accomplishment Information*" section on an FD-542 is a function of the macro. If the FD-542 is selected, the "*Accomplishment Information*" will automatically be placed on the last page of the document and consists of; the number of accomplishments claimed, type of accomplishment, investigative technique used, and information on the person claiming the accomplishment(s).

FD-542 Copy Count: (Same as EC above)
*Note: Document type on an FD-542 is "**.542**"

Example 4


To: San Antonio From: San Antonio
Re: 300C-SA-C50782, 04/18/2005

Accomplishment Information:

Number: 1
Type: POSITIVE INTELLIGENCE (DISSEMINATED OUTSIDE FBI)
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN: 123456789
Name:
Squad: A11

10Bjljp02.gth

b6
b7C

FD-71 (Complaint Form):

The purpose of the FD 71 is to document complaints received via:

- Telephone
- Walk-in
- Letters
- Faxes
- E-mail
- Other agencies

***IT/DT complaints are handled through the Guardian system.

FD-71 Copy Count: **1** (Same as EC above)

FD-302 (Report Discoverable Information):

The purpose of the FD-302 is to document discoverable information (i.e. information that you may have to testify to in court)

FD-302 applications: (examples)

- Documenting when accepting or providing evidence
- Documenting interviews
- Documenting results of surveillance
- Documenting subpoena results
- Document results of trash runs
- Document arrest

FD-302 Copy Count: **2**

First copy (same as EC above)-

Second copy (clean! i.e. **No** initials, **No** **Red** marks, **No** Julian date, **No** indexing)

FD-320 (Notification to DOJ):

The purpose of the FD-320 is to notify the Department of Justice of a case closure. It is completed after approval from the JTTF Supervisor and consultation with the Assistant United States Attorney assigned to the case.

FD-320 Copy Count: **3**

First copy

- ✓ White paper: Clean with no markings (i.e. no initials or copy count) This copy is for the U.S. Attorney's Office
  - It can be mailed to: *U.S. Attorney's Office*
    Attn: AUSA XXXXXXX
    Address: _____
    _____
    _____
  - It can also be given to your JTTF AUSA

Second copy (Original)

- ✓ This copy must be on **Yellow paper** with **copy count* on lower left corner.
- ✓ Put Check mark in **Red Ink** next to the Case ID
- ✓ Initialed in **Black Ink** next to your typed initials.

Third copy (Your Serialized Copy)

- ✓ This copy must be on **Yellow paper** with **copy count* on lower left corner.
- ✓ Same as Serialized Copy on EC, FD-542, Etc. above

(**copy count* includes your *Case ID*, your typed *initials* and the *number of copies.*)

Example copy count: 266F-NY-55619
PAH:pah (use your initials)
(3)

FD-515 (Statistical Accomplishment)

The purpose of the FD-515 is to claim what is referred to as a "hard stat." **The FD-515 **MUST** be completed within **30 days** of the event**

FD-515 applications:

- ➢ Complaint/Information/Indictment
- ➢ Arrest
- ➢ Conviction
- ➢ Sentencing
- ➢ Asset seizure
- ➢ Other

FD-515 Copy Count: **1**

FD-930 (Violent Gang and Terrorist Organization File)

The purpose of the FD-930 is to nominate a subject of International or Domestic Terrorism for inclusion on the Terrorist Watch-list.

FD-930 applications:

- ➢ Nominate a subject for inclusion on the Terrorist Watch-List.
- ➢ Remove a previously nominated subject from the Terrorist Watch-list.

FD-930 Procedures:

- ✓ Complete FD-930 e-form (*See 'Tips for completing the FD-930 e-form' below)
- ✓ After completion, *validate* the FD-930 e-form by clicking on the **"Validate Form"** button at the top of the screen.

*If the form was completed with valid data and all required fields have been populated, the red **'NOT VALID'** indicator will turn to a green **'VALID'** indicator. If the form was not completed with valid data and/or all required fields have not been populated, the red **'NOT VALID'**

indicator will remain and a window will appear listing all invalid data and/or omitted fields that need to be addressed by the Case Agent before the form is submitted to the TREX Unit. Field Offices should not upload either 'VALID' or 'NOT VALID' FD-930s into ACS. The TREX Unit will be responsible for function.

- ✓ Save the completed FD-930 to a file/folder of your choice.
- ✓ Prepare an e-mail to HQ_DIV13_TREX, with the subject line of the e-mail being your substantive investigative case file number, and attach the completed FD-930 e-form. Based on the 'Type of Request', the following documents **must** be sent as attachments to the e-mail submitted to HQ_DIV13_TREX:
  - If the 'Type of Request' is 'Initial Submission': FD-930 **and** opening case EC **and** NOI or LHM.
  - If the 'Type of Request' is 'Remove Individual from ALL Watch-listing and Supported Systems': FD-930 **and** closing case EC.
  - If the 'Type of Request' is 'Add Data to Existing Record' or 'Modify or Delete Data From Existing Record': FD-930 **and** EC clearly stating what is to be added to, deleted from or modified in the existing record.
- ✓ TREX Unit will review the nomination for thoroughness and accuracy, reconcile all conflicting issues, and make appropriate notifications (TSC, NCTC, etc.). The TREX Unit will then send an e-mail to the Case Agent containing a copy of the completed FD-930 that has been uploaded to the substantive investigative case file, and the serial number of that document.
- ✓ Print one (1) hard copy of the e-mail for uploading/serializing into the substantive case file.
- ✓ Print two (2) copies of the FD-930, one (1) for the substantive case file and one (1) for the VGTOF control file.

Tips for completing the e-form FD-930:

- ➢ Mandatory fields are highlighted by red asterisks or red borders. Some fields become mandatory when a condition is created, *i.e.*, when the 'Type of Request' is 'Initial Submission' or based on the subject's U.S. Person status.
- ➢ Holding the cursor over some fields will display a window with tips for properly completing the field.
- ➢ Drop-down menus/pick-lists may be accessed by clicking on the downward arrow located on the right side of the field. (The first line in all drop-down menus is blank and should be selected if the field is inadvertently populated. This will depopulate the field.)
- ➢ Add Additional...' lines are directly below base fields for any biographical data element for which multiple entries are accepted. i.e., date of birth, social security account number, scars/marks/tattoos/other characteristics, etc. By single clicking on the 'Add Additional...' line another field will appear and allow for additional data elements to be entered.

- When certain conditions are created on the form, pop-up windows will appear advising the Case Agent of a conflict. For example: If a subject has been determined to be Armed and Dangerous and the Armed and Dangerous caveat is entered as a Caution and Medical Condition, the subject may not be issued a Silent Hit Handling Code. Law enforcement officer safety is paramount; therefore, initial eligibility criteria for an individual to be issued a Silent Hit Handling Code is that the individual may not pose a safety or violence threat to law enforcement.
  Policy and procedural ECs cited on the form may be directly accessed by clicking on the communication's reference link.

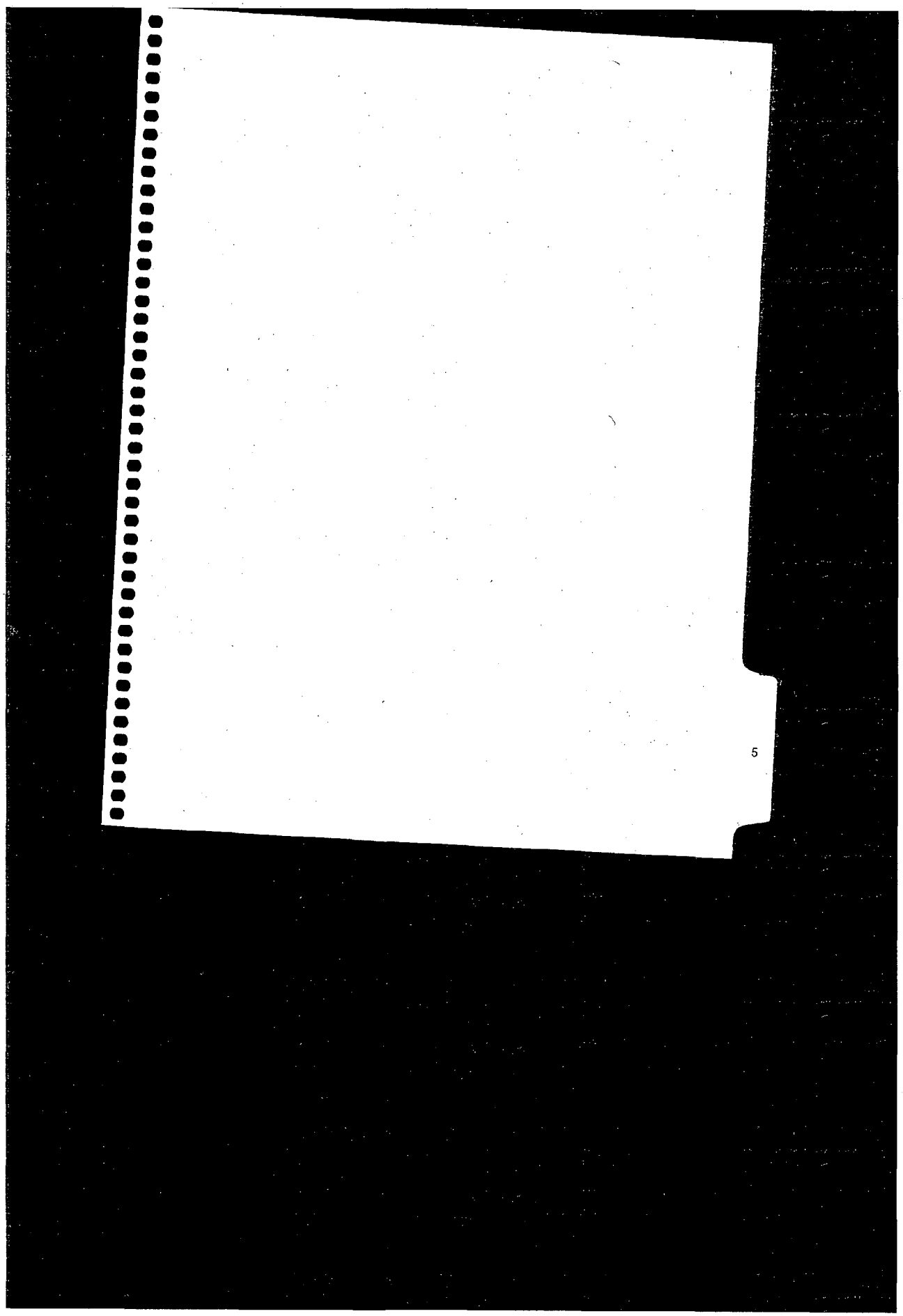
LHM (Letterhead Memorandum)

The purpose of the LHM is to notify various departments, including the Department of Justice, Office of Intelligence Policy and Review (OIPR) and FBIHQ, of your intent to open an intelligence case. The initial LHM must be accompanied by an Opening EC.

LHM Copy Count: 2

First Copy
- ✓ White paper: clean! (i.e. **No** initials, **No Red** marks, **No** Julian date, **No** indexing) For the file attached to the EC.

Second Copy (with attached EC to FBIHQ substantive desk SSA)
- ✓ Initialed in **Black Ink** next to your typed initials.


5

INVESTIGATIVE PLAN:

ALL INVESTIGATIONS MUST BE APPROVED / ASSIGNED BY THE SQUAD SUPERVISOR AND CONDUCTED IN ACCORDANCE WITH THE ATTORNEY GENERAL GUIDELINES.

1. **RECEIVE COMPLAINT:** Complaints can come from many sources including, but not limited to:

   - FD-71
   - Electronic Communication / Lead
   - Telephone call
   - E-mail
   - Local Police Department Report
   - Guardian
   - *Assessment

   *(*An Assessment is a proactive collection of information concerning threats to National Security, including information on individuals, groups and organizations of possible investigative interest)*

   A complaint is marked based on the deadline by which it must be completed:
   - **Immediate – 24 hours**
   - **Priority – 72 hours**
   - **Routine – 60 days**

2. **CREATE A WORKING FOLDER:** As you begin conducting an investigation the volume of information can be overwhelming. A good working folder is vital to maintaining and organizing this information as it comes in. Although there are no rules on what can be maintained in a working folder, some examples of information that ***should*** be included are:

   - Results of Data-Base Searches
   - Photos
   - Copies of all Documentation (EC's, FD-542's, FD-302's, Surveillance Logs)
   - Copies of all Subpoenas / National Security Letters
   - Information on Related Cases

3. **CONTACT COMPLAINANT: (if appropriate)** Although the original complaint ***should*** contain all necessary information, the reality is that this ***may not*** always be the case. If the original complaint is lacking necessary or sufficient information, now is the time to re-contact the complainant and "fill in the blanks". Examples of relevant information that may not have been included in the original complaint are:

   - Subject's **Full** Name
   - Physical Description
   - Identifying Numbers (Social Security, Drivers License, Passport)
   - Telephone Numbers
   - Complete Address
   - Other Relevant Details of the Specific Incident

4. **CONDUCT DATABASE CHECKS:** *(See your JTTF's Investigative Check List, if applicable)* A Standard of Investigation is required to ensure that each and every complaint is properly investigated. The Standard of Investigation will vary, but may include approximately 25 investigative databases, and every Investigator **should utilize each and every database when applicable.**

   It should also be noted that this checklist (if applicable) is ***not all inclusive*** and ***should be considered a minimum.*** Investigators should feel free to incorporate other relevant database checks that may not be included on their JTTF Investigative Check List.

   Important Considerations when Conducting Database Checks:

   - Investigators should seek the assistance of other Task Force Officers, Special Agents, Intel Research Specialists (IRS), Investigative Assistants (IA), and/or Intelligence Analysts (IA) to run these checks.

   - When checking Local Law Enforcement involvement, Investigators are reminded to also run checks with the Agency that has jurisdiction where the subject resides, to include past or historical residences.

   - Include both **positive** and **negative** results within your working folder.

5. **DISCUSS COMPLAINT STATUS WITH SENIOR TFO/AGENT:** Although you may already have a good idea of the complaints case potential at this point, you should discuss the results of the database checks with a Senior TFO/Agent. This will provide an outside perspective, which can be invaluable, but will also insure that you have not overlooked a tool or technique that *could* or *should* have been utilized.

Important Considerations when Discussing Complaint Status:

- Determine the validity of the complaint
- Discuss additional tools or techniques that could be utilized at this stage
- Determine if the Subject of the complaint should be contacted and interviewed
- Determine if the Lead or complaint is sufficiently covered
- Determine if a Preliminary Investigation or Full Field Investigation should be initiated

**If it is determined that the Guardian lead is sufficiently covered, it can be closed, within Guardian.*

If it is determined that the Guardian lead is **not sufficiently covered and that further investigation is warranted, continue with "INVESTIGATIVE PLAN", step 6, below.*

6. **INITIATE PRELIMINARY INVESTIGATION OR FULL FIELD INVESTIGATION:** Before opening a *case*, you must first determine whether a *Preliminary Investigation (PI) or *Full Field Investigation (FFI) is warranted. Once the case level is determined, complete the appropriate paperwork as outlined under *"REQUIRED DOCUMENTATION" in Tab 4"*.

Important Considerations when Opening a PI or FFI:

- You must obtain approval from your Supervisor to open a case
- Determine if a Co-Case Agent should be assigned
- Begin to develop a detailed investigative plan, based on the Criminal Activity suspected
- Assign support duties and responsibilities when needed (i.e. assistance completing opening paper-work, issuing subpoenas/NSLs, sending *Leads* to other field offices, Surveillance requests/planning/conduction, etc.)
- Make necessary changes to your *working folder*. (Your *complaint working folder* may not be sufficient for the volume of information associated with a PI or FFI)
- Periodically, during the course of the investigation, brief your Supervisor regarding the *case status* and *direction*.

***Preliminary Investigation*:**

*Standard - There is information or an allegation indicating that a threat to National Security **may** exist.*
Authorized Techniques - A general summary is provided in Tab 3-"Legal Application". (See Attorney General Guidelines for complete authorization)
Duration - Six months (with extensions granted under certain circumstances)
Approval Authority - SSA grants initial opening . SAC may grant an extension for an additional six months. Extensions in excess of one year require FBI HQ approval.

Full Field Investigation:

*Standard - There are **specific and articulable facts** giving reason to believe that a threat to National Security **may** exist.*
Authorized Techniques - A general summary is provided in Tab 3-"Legal Application". (See DIOG reference slides below, or full DIOG on FBInet)
Duration - Indefinite, with a required Annual Letter Head Memorandum (LHM).
Approval Authority - SAC is the approval authority.

For study materials related to the Domestic Investigation and Operations Guide, see the following link:

http://home.fbinet.fbi/forms/fd1028/DIOG/DIOGTraining/Trainee%20Materials/Forms/AllItems.aspx

USE AND APPROVALS FOR INVESTIGATIVE TECHNIQUES

A. **Polygraph Matters:** Authority granted by the ASAC, unless unusual or special circumstances exist, i.e. a request to polygraph a minor, etc, for which approval would be granted by the SAC. For your Division polygrapher(s) see your contact list or JTTF Coordinator

B. **Consensual (telephonic) Monitoring:** Approval granted by ASAC. If sensitive circumstances exist, as defined on from FD-759, approval will be granted by the SAC.

1. Consenting party must sign FD-472
2. Obtain concurrence from your AUSA that recording is legal and no entrapment issues exist. Document same on an FD-320 (for CW's obtain the authority prior to opening and gain concurrence for the duration of the investigation)
3. Draft FD-759 (now a macro) and forward to ASAC for authority. In the event that consensual recording needs to take place immediately contact SSA and ask that he/she call the ASAC for verbal authority. Once verbal authority is granted, document same on the original FD-759.
4. Two Agents or an Agent and a TFO/TFA must be present during the recording.
5. Record a preamble on the tape (date, time, witnesses, number called and name of the subject called)
6. Record a post amble at the conclusion (time call ended, call not answered/answered/ answering machine, etc)
7. Label the tape
8. Must submit tape to ELSUR within 10 days. Use the FD-504(b) evidence envelope (1D evidence), fill it out and submit it to your ELSUR contact. If a CW is utilized to place the call, his/her true name is listed on the subject intercepted line along with the intended interceptee.
9. Document the consensual call on an FD-302. The FD-302 will essentially be your debrief of the CW following the call (briefly include the pertinent content), document that the call was a consensual recording and the tape submitted into evidence. Remember that the tape is the evidence and the transcript is your guide for the jury to follow the conversation word for word.

C. **Consensual (non-telephonic) Monitoring:** ASAC will approve authority via FD-759 for routine monitoring and for emergency monitoring (sensitive circumstances) when a designated DOJ official cannot be reached for approval.

When sensitive circumstances exist, routine non-telephonic authority is granted by DOJ seven days prior to the monitoring.

Consensual monitoring outside of your division may be conducted only after prior notification to and concurrence obtained from the SAC of each division where monitoring will occur. You must document the concurrence. An AUSA advisement that the monitoring is legal and appropriate is necessary only in the judicial district which encompasses the office of origin of the investigative case.

1. Consenting party must sign FD-473
2. Obtain concurrence from your AUSA that recording is legal and no entrapment issues exist. Document same on an FD-320 (for CW's obtain the authority prior to opening and gain concurrence for the duration of the investigation)
3. Draft FD-759 (now a macro) and forward to ASAC for authority. In the event that consensual recording needs to take place immediately contact SSA and ask that he/she call the ASAC for verbal authority. Once verbal authority is granted, document same on the original FD-759.
4. Two Agents or an Agent and a TFO/TFA must be present during the recording.
5. Record a preamble on the tape/digital recording device-F-bird, Eagle-(date, time, witnesses, number called and name of the subject being recorded)
6. Record a post amble at the conclusion (time recording ended, etc)
7. Label the tape at the conclusion. If using a digital recording device download the recording onto a CD-ROM.
8. Must submit tape and/or CD-ROM to ELSUR within 10 days. Use the FD-504 evidence envelope (1D evidence), fill it out and submit it to your ELSUR contact. If a CW is a recorded party, use his/her true name on the subject intercepted line along with the intended interceptee.
9. Document the consensual recording on an FD-302. The FD-302 will essentially be your debrief of the CW following the recording (brief, include the pertinent content; who, when, where, what was discussed), document that the call was a consensual recording and the tape/CD-ROM submitted into evidence. Remember that the tape/CD-ROM is the evidence and the transcript is your guide for the jury to follow the conversation word for word.

D. **Taping of Interviews and/or Confessions:** Approval to tape interviews and or confessions may be granted by the ASAC. If taping will be done without the consent of the interviewed party, authorization must be documented on an FD-759, with the interviewing agent being the consenting party.

E. **Closed Circuit Television (CCTV):** All consensual CCTV authorization (FD-759) will be approved by the ASAC. Follow the procedure listed above in #2 and #3 for handling the evidence and documenting the recording.

F. **Public Area Viewing/Pole Cameras:** Authorization (FD-677) in which a court order is not required will be approved by the SAC or the Acting SAC.

1. An FD-871 must be submitted for the assignment of a Technically Trained

Agent. See your contact list or JTTF Coordinator regarding these submissions. After you complete the request, the form will automatically be generated and forwarded the tech agents so they can make their preparations. Route the original to the CDC and SAC for signature (noted on the bottom of the FD-871). Retain a copy for your file.

2. Do a site survey for the Tech Agents. Relay any safety issues and counter-surveillance concerns associated with your subject.

G. **Group II UCO:** Will be reviewed by the Division Undercover Review Committee and signed by the Division UC Coordinator, CDC, and the appropriate ASAC prior to submission to the SAC for approval.

H. **Group I UCO:** Will be reviewed by the Divisions Undercover Review Committee and submitted to the SAC with recommended action (Group I UCOs submitted to the SAC should include U.S. Attorney approval letter)

I. **Purchase of Drug Evidence:** Approval granted by the ASAC via EC.

1. Fill out FD-794 requesting "drug purchase funds" and forward with approval EC.
2. [redacted] b7E

Document this in your FD-302--In addition [redacted] -Document this in your FD-302).

3. Following the transaction, the receipt must be returned and filed (consult your JTTF Coordinator or SSA for division-specific procedures). Keep a copy of the receipt for your records.

J. **Administrative Subpoenas (Title 21 Investigations ONLY--Drug Cases):** Authority to compel attendance and testimony of witnesses, and require records production relevant to controlled substance investigations may be granted by your SSRA, OC/DP SSA, or ASAC.

K. **Mail Cover:** Approval is with the SAC or in his/her absence, the Acting SAC. (Review Ponies for Mail Cover)

L. **Pen Registers/Trap and Trace:** Approval granted by the ASAC (Court order or consent of user is required).

1. Identify the subscriber prior to seeking approval (if possible) via Federal Grand Jury (FGJ) Subpoena, Administrative Subpoena or National Security Letter (NSL).
2. Draft Approval EC (See pony)
3. Tech Request FD-871, follow procedure in #6, sub a

4. Draft Application and Order (See pony). Allow AUSA to review, have Orders signed by Magistrate Judge. File with the Clerk of Courts
5. Copy to substantive case sub-file (will be opened by your rotor).
6. Copy to Tech Agent--will be faxed to service provider
7. Additional copies, as applicable, along with a signed copy of approval EC. The appropriate personnel receiving these copies should upload your call data into Telephone Applications and send you a hard copy of the pen raw data.
8. Open a sub-file for your raw data. Name it "Rawdata 1", or something along those lines.
9. [redacted] b7E
[redacted] Make sure the data is captured by your pen register and document same in an FD-302.

M. **Title III Electronic Surveillance (Non-Sensitive):** Approval will be granted by the SAC (via EC) or in his/her absence, the Acting SAC. The authority cannot be delegated lower that an ASAC serving as Acting SAC.

1. Pen Register(s) should be up and running unless you are requesting emergency authority. Analyze the raw data routinely; use the information to identify individuals possibly involved in the specified illegal activity.
2. Before you draft an Affidavit, make sure that you have exhausted all other investigative techniques and have specific examples of why a Title III is the only technique that will meet your investigative goals. Make a copy of an FD-699 (Title III Checklist)
3. Draft EC seeking approval from your SAC (See pony).
4. Draft Affidavit (See pony). Make sure that your AUSA is on board and the United States Attorney's Office supports the technique.
5. Tech Request (FD-871). Follow the same procedure for getting the request form to the Tech Agent..
6. EC requesting Pre Title III ELSUR checks (See pony). Make sure that all target telephone numbers, target subscriber addresses, ESN'S, etc., as well as Named Interceptees are checked through the databases. Remember that the ELSUR checks are only good for 45 days. Do not do them too early in the process and do not do them to late, DEA and BICE have a 5 day window to conduct the searches.
7. When your Affidavit is complete, provide a copy to your SSA, the CDC and your AUSA for review. Make appropriate changes, additions and/or deletions as needed to your Affidavit. The AUSA will draft the Application and Order (send copies of the drafts to your CDC, for ELSUR purposes).
8. When the Affidavit, Application, and Order have been reviewed and approved by the CDC and AUSA, they will be forwarded to OEO for the next approval. When approved, an Action Memo will be drafted and approval granted. Make sure your Tech Agent knows where you are in the

process and the appropriate equipment has been installed before you have the Order signed by the Judge.

9. Draft an EC requesting that appropriate subfiles are opened.

   a. -ELA---ELSUR Administrative
   b. EL1----ELSUR Original Log
   c. EL1A--ELSUR Copies of Log
   d. EL1B--ELSUR Transcripts

10. AUSA will draft Minimization Instructions. Set up a meeting with all monitors, AUSA, SSRA/SSA, and Case Agent. Everyone must read the Affidavit, Application and Order. Go over minimization instructions and everyone will sign a copy of a log documenting same.
11. Application, Order, Affidavit to Federal Judge for signature. Make sure copies make their way to the substantive file, Tech Agents, ELSUR, etc.
12. Seal tapes/CD's at the conclusion of Title III. AUSA will draft a Sealing Order and you, the AUSA, and the original tapes/CDs will go to the Judge for sealing of the evidence. Make sure the original evidence is submitted to ELSUR within 10 days. Make sure a copy of the Sealing Order makes its way to the appropriate sub-file.

N. **Federal Grand Jury Subpoenas:** Open a case predicated upon allegations of criminal activity. Fill in a FGJ request form (See Pony) and forward to your AUSA or his/her secretary.

1. Sign your 6e letter (drafted by the USAO) and return. Maintain a copy for your records.
2. Serve the subpoena. Fill out the back of the subpoena that is to returned to the USAO and get it there. Maintain a copy for your file (GJ subfile in your case--will be opened by your rotor).
3. Pick up the requested documents and/or information and document the receipt via FD-302.
4. Make your returns through the USAO.
5. If the records will be reviewed by other TFOs, TFA, or Agents, make sure that everyone has signed a 6e letter. Send the original to the USAO and copies of the letters to your GJ sub-file.
6. Some service providers will accept FGJ Subpoenas via fax. If not, set a lead for the appropriate division to serve the subpoena.

O. **National Security Letter:** [redacted] Approval authority granted by SAC (Acting SAC cannot sign an NSL).

1. Draft NSL and EC through [redacted] b7E
2. Populate pertinent [redacted] form information for EC and NSL.
3. EC and NSL will be automatically generated by [redacted] and routed to your SSA, ASAC, CDC, and SAC for review and approval..
4. Type an FD-542 claiming statistical accomplishments for drafting and approval of NSL.

5. [redacted] b7E

6.

P. **Foreign Intelligence Surveillance Act (FISA) procedures:** Download a FISA Request Form from the OGC/FISA Unit webpage in FBInet (business records, Pen Register/Trap and Trace, Full FISA). The request form must be downloaded and completed. (Note: [redacted]

1. Initiate the FISA process through the [redacted] During this process, you may expect the following tasks:

a. [redacted] b7E
b.
c.
d.
e.

*Expect a two or more month lead-time in the completion of these steps.

THE FBI FISA PROCESS: FFI INITIATION APPLICATION PACKAGE FISC REVIEW HEARING COURT ORDER

2. When the Application and Order make it through the gauntlet, fill out a Woods Form. When the appropriate checks have been conducted secure fax the document to FBIHQ.

*In addition to the existing "Sub FISA" created for each investigation, a sub-file containing the materials relied upon to verify the items on the "Woods" checklist must also be created and maintained by the case agent. This sub-file must be created for each FISA application submitted and named "Sub Woods Checks". It will contain the results of all material relied upon in the "Woods" verification procedures.

**Application prepared by OIPR and signed by the AG
**Declaration sworn to by FBI agent from FBIHQ substantive unit
**Certification signed by the FBI Director.
**Electronic surveillance order
**Supplemental order to service provider
**Supplemental minimization procedures (rare)

3. FBIHQ will usually send supplemental orders to the division where the service provider is located. Make sure that copies make it to the substantive file and your Tech Agent. The Tech Agent should ensure that the appropriate personnel get an unclassified document requesting that they upload the raw data into Telephone Applications.

4. Open a subfile for your pen register raw data (See the Pen Register summary).

a. FISA RENEWAL REQUESTS

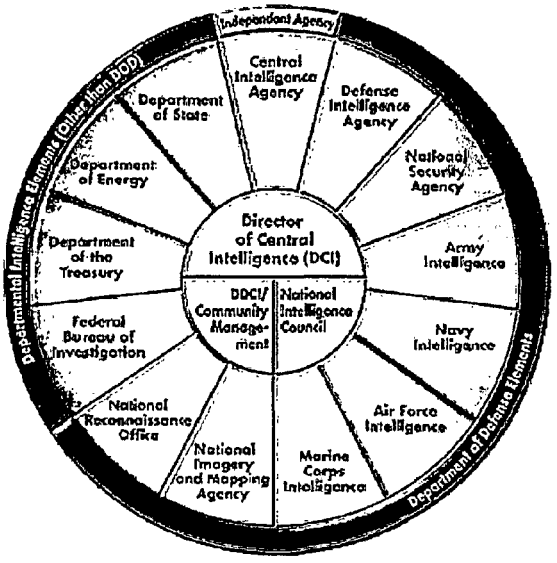
i) Draft a request form, type in the Docket Number from your original order and check the renewal box. Provide information that you have developed during the 90 days of operating (PRTT analysis, surveillance, etc) in the body.

ii) The signature authority needed for the FISA Request Form.

iii) Upload your request into the FISA Management System on the Intranet.

INTELLIGENCE INFORMATION REPORT

Intelligence Community



PURPOSE

As a result of 09/11/2001, the FBI has massively intensified its intelligence dissemination effort. The FBI has historically limited its intelligence sharing through established Intelligence Information Reporting channels normally used by the 15-member United States Intelligence Community (USIC). As the leading domestic criminal, counterintelligence and counterterrorism agency, the FBI has adapted its reporting to facilitate the rapid dissemination of its raw intelligence. The Intelligence Information Report (IIR) is the primary vehicle for this dissemination.

The IIR is the standard through which all "raw" or unevaluated intelligence information is shared with national policy makers, the USIC and law enforcement community in support of national intelligence priorities and the needs of law enforcement consumers. These reports are primarily used by analysts and agents, along with other available sources, to identify threats or trends, and produce finished intelligence products for consumers. As a result of this reporting and eventual analysis, national strategies and action may be affected.

A significant benefit to analysts and agents using the IIR as a dissemination tool is the ability to protect the source of the information while providing essential raw intelligence. This information sharing will also enhance the FBI's collection efforts and support the war on terrorism in accordance with national directives:

It is the responsibility of the FBI to share terrorism intelligence and it is mandated by the National Security Act of 1947, Executive Order 12333, the USA Patriot Act, the Homeland

Security Act of 2002, and the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection.

Historically, counterintelligence and counterterrorism asset reporting primarily fueled the IIR process. However, criminal and cyber source reporting is now being incorporated to broadly share information across all FBI investigative program lines. Intelligence harvested through investigative techniques such as Foreign Intelligence Surveillance Act (FISA) and Title III overhears, consensual monitoring, physical surveillance, as well as other sophisticated techniques, can also be the basis for raw intelligence disseminated through IIRs.

Intelligence collection is the responsibility of all personnel who investigate or support investigations. These include agents, task force members, language specialists, Intelligence Analysts (IA's), financial analysts and surveillance group members. To facilitate the IIR process, these personnel must become familiar with the National Humint Collection Directives (NHCD's) and the FBI's Intelligence Collection Requirements (ICR's) pertinent to the programs and countries they are working. The NHCD's list the exact issues of interest to the USIC and establish parameters for positive or foreign intelligence reporting. The ICR's focus the FBI's intelligence collection efforts and fill intelligence gaps. The aforementioned investigative personnel must be vigilant and identify relevant intelligence derived from asset reporting, intercepts, surveillance observations and information uncovered from other sophisticated technique collection platforms.

Task force members who produce IIRs based on information available to them through their task force assignment should follow the below protocol to process their IIRs. These IIRs need to go through FBI channels with a notation made on the administrative "tickler" page giving the task force member and their respective agency credit. Additionally, task force members should coordinate with their agency to ensure their efforts are credited within their organization.

Your divisio

b7E

To further facilitate the timely entry and dissemination of information deemed suitable for IIR dissemination, Senior Reports Officer positions have been established within field offices. These Intelligence Analysts have the capability to bypass approving officials at HQ and directly disseminate timely IIRs. All agents or Task Force

Officers identifying information suitable for IIR dissemination should follow the below listed protocol.

PROTOCOL

1. All agents should review every document they produce for intelligence value and consider submitting the information to the [redacted] for review.

2. All agents should forward documents (ECs, FD-71s, FD 302s, FD 542s) they believe have IIR potential to their division [redacted] or JTTF IA.

3. The IIR Manager or th[redacted] supervisor must be contacted by phone if the data contains specific threat information which must be reported within two hours (IMMEDIATE IIR). If the information contains specific threat data, both the reporting agent and their supervisor must remain available until the report has been received at FBIHQ and then either published or rejected by FBIHQ. b7E

4. While the [redacted] will prepare IIRs, assessments and bulletins using the intelligence you provide, each agent and supervisor is still responsible for preparing Urgent Reports (if necessary) and contacting other divisions, squads, Legats, or agencies to alert appropriate personnel regarding the information.

5. The IIR Manager will review the IIR material and determine which program it addresses (CT, FCI, CRIM, or Cyber). The IIR will then be assigned to an Intelligence Analyst (IA) for action in accordance with division protocols.

6. The IA will draft an IIR on-line, using the FBI Intelligence Information Report Dissemination System (FIDs) and examine the IIR for content, format, and compliance with FBIHQ procedures. The IA will also redact names of US Persons, ensure sources and methods are protected, and correlate the reported information with the FBI's Intelligence Requirements.

7. The IA will e-mail a PDF version of the Draft IIR to the agent and the squad supervisor, with the following message:

   "Attached is your draft IIR for review and approval."

8. As part of the review and approval process, it is the agent's responsibility to:
   a. Ensure that information in the IIR will not jeopardize any sources or methods or adversely affect an ongoing case.
   b. Have his supervisor review and approve the IIR, or recommend changes.

9. The agent can either accept the draft or request changes. Any changes to the IIR must be coordinated with the squad supervisor. Corrections should be addressed

in an e-mail format to the IA. If no corrections are needed, paragraph 11 applies.

10. If corrections are requested, the IA will make the corrections and e-mail a corrected copy of the IIR to the agent and supervisor for approval.

11. The agent and squad supervisor should e-mail the IA once the IIR is approved. An IIR will not be submitted to FBIHQ without the agent's and supervisor's approval. In exigent circumstances, verbal approvals are acceptable, but must be followed up with a confirmation e-mail.

12. Through FIDS, the IA will forward the approved copy to the [redacted] supervisor, who will be the final approval authority in the Division for ROUTINE and PRIORITY IIRs. IMMEDIATE IIRs must be approved by an ASAC. b7E

13. The IIR will then be transmitted to the appropriate FBIHQ component, using FIDS. After forwarding the IIR for approval in FIDS, the IA will e-mail the agent the final copy of the IIR, in a text format for uploading into ACS.

14. The agent should then save the renamed text version final IIR to his draft folder.

15. The agent will print copies (one copy for each file referenced in the admin portion of the IIR, and one copy for indexing of the IIR), have his supervisor initial the bottom of the IIR, and forward the IIR to his SST for uploading.

16. If an IIR was produced with information provided by a source or asset, one copy of the IIR should be blind copied to the source or asset main file only, not the sub-A. A copy of the IIR should also be e-mailed to either the blue or green file.

17. The agent should claim a Statistical Accomplishment using the FD-542, and FD-209 if the information within the IIR was obtained by a Source.

*** Further guidance on the production and dissemination of IIRs can be found by searching the Directorate of Intelligence→ Domain and Collection Management Branch→ Reports Section on FBInet, or by consulting your FIG.

*If an agent elects to disseminate a hard copy of the IIR to a local agency with appropriate clearance, the administrative section of the IIR **must** be removed.

PONIES, FORMS, and EXTRAS

The Following 'Ponies' and 'Resources' are lists of documents you may need in the course of your duties. Field Division-specific ponies may be found on your office's share drive. You can also search for particular ponies at:

- **Production Services Unit (PSU)- Includes guidance on understanding and producing intelligence products.**
  http://home.fbinet.fbi/NSB/DI/ab/fips/PSU/Pages/Default.aspx
- **International Terrorism Operations Section I (ITOS I)- Includes numerous ponies for the most common CT documents.**
  http://home.fbinet.fbi/NSB/CTD/ITOSI/Pages/OPtemplates.aspx

...or by doing an Intranet search for "ponies".

***IMPORTANT: Please do not alter original *Ponies* or *Resource documents*, contained in the common (S:) drive, as this will make them unusable to other personnel. Before making any changes, you must first re-save the document to your personal folder, under a different name.**

EC (Electronic Communications):

Preliminary Investigation
- Opening Preliminary Investigation
- Opening Preliminary Investigation (TEI)
- Extension of a Preliminary Investigation
- Convert Preliminary Investigation to Full Field Investigation
- Closing Preliminary Investigation

Full Field Investigation
- Opening full Field Investigation
- Closing Full Field Investigation
- Annual Summary

Criminal Case
- Opening Criminal Case
- Closing Criminal Case

Leads
- Reporting Lead Covered
- Sending Lead Outside Your Division

Evidence
- Destruction of Evidence
- Explanation for Late Submission of Evidence
- Return of Evidence

Title III

- Title III Approval
- Title III Authority
- Title III-ELSUR Checks

Request Assistance

- Request CART Assistance
- Request Communication Analysis Unit Assistance
- Request for Information from NSA
- Request IRS Information
- Request Laboratory Assistance
- Request Polygrapher

Asset

- Approval
- Cover
- JTTF-TFO Authorization
- Opening
- Undisclosed Participation

Miscellaneous

- After Action Report
- Change Title/Case ID
- Mail Cover
- Opening a Sub-File
- Operational Plans
- PRTT Authority
- Reporting Accident
- Sending Documents to the File
- Source Canvas
- Submitting Letter-Head Memorandum
- Transfer a Case to Another Agent/TFO
- Travel Outside Division
- VGTOF Entry

FD-542:

Surveillance

- Request Surveillance [redacted] b7E
- Conducting Surveillance [redacted]

National Security Letter

- Preparation and Approval of a National Security Letter
- Serving a National Security Letter

Participating in an Event
- Participating in Command Post/Major Case/Special Event
- Participating as a Member of a WMD Working Group/Task Force

Miscellaneous
- Dissemination of information
- LEA Liaison

FD-302:

Miscellaneous
- Receiving Evidence
- Receiving Subpoena Results
- Conducting Interview
- Conducting Surveillance
- Conducting Trash Cover
- Making an Arrest
- Arrest Log

LHM (Letter-Head Memorandum):

Asset
- LHM
- Notification LHM

Miscellaneous
- Annual Summary
- IRS Information Request
- Opening an Asset
- Opening Full/Preliminary Investigation
- Request for Access
- Request Information
- Subpoena Service

NSL (National Security Letter):

Request for Emergency Disclosure of Information

ECPA E-mail Subscriber
- ECPA Checklist
- E-mail EC
- E-mail NSL

ECPA E-mail Transactional Records
- ECAP Checklist
- Transactional EC
- Transactional NSL

ECPA Telephone Subscriber
- ECPA Checklist
- Subscriber EC
- Subscriber NSL

ECPA Toll Billing
- ECPA Checklist
- Toll EC
- Toll NSL

FCRA Consumer Identifying and Financial Institutions Info.
- FCRA Checklist
- Combination Credit EC
- Combination Credit NSL
- Experian EC

FCRA Consumer Identifying Information
- FCRA Checklist
- Credit (b) EC
- Credit (b) NSL
- Experian EC
- Experian NSL

FCRA Financial Institutions
- FCRA Checklist
- Credit (a) EC
- Credit (a) NSL
- Experian EC
- Experian NSL

FCRA Full Credit Report
- Credit Report Checklist
- Credit Report EC
- Credit Report NSL
- Credit Report Instruction EC

RFPA Financial Records
- RFPA Checklist
- Bank EC
- Bank NSL

Miscellaneous Forms:

Search Warrant
- Search Warrant Cover

- Search Warrant Affidavit
- Search Warrant Application

Seizure Warrant
- Seizure Warrant Cover
- Seizure Warrant Affidavit
- Seizure Warrant Application

Surveillance
- SOG Request Form
- Surveillance Log

FISA
- FISA Request Form PRTT
- FISA Request Form

Title III
- ECTIII Approval
- TIII Affidavit

Miscellaneous
- ECPRTT Authority
- Case Status Form (FD-320)
- Case Update Example
- Notification of Authority to use Monitoring Equipment (FD-759)
- Tax Return Application
- Technical Request Form (FD-871)
- NCIC Initial Entry (FD-65)
- Non-Compulsory Letter
- Pen-Trap Application and Order
- Urgent Report-Guidelines & Format
- Arrest Plan
- Arrest Warrant
- Attestation of Authenticity of Foreign Public Documents
- Attestation with Respect to Seized Articles
- Certificate of Authenticity of Business Records
- Complaint Affidavit
- Criminal Complaint
- Evidence Description
- Evidence Records Access Sign In/Out Log
- FD-930/Violent Gang and Terrorist Organization File (e-form)
- FISA Request Form PRTT
- FISA Request Form
- Investigative Support Specialist Information Request Form
- Request for Emergency Disclosure of Information
- Room Access Sign In/Out Sheet

- Translation Request Form (TRF)
- Woods form

Subpoenas

- Airlines
- Automobile Dealerships
- Bail Bond companies
- Bank Account Information
- Bank Comprehensive
- Bank Financial Records
- Bank General Records
- Casinos
- Corporation-Detailed
- Corporation General
- Credit Bureau
- Credit Card Records-Detailed
- Credit Card Records
- Electronic Records Request-General
- Escrow Company
- Hotel Records
- Insurance Companies
- Lawyer Fee Records
- Real Estate Broker
- Retail Stores
- Securities Broker
- Telephone Company-Cellular
- Telephone Company-General
- Telephone Long Distance Provider
- Travel Agency

TERRORISM STATUTES THAT GRANT INVESTIGATIVE JURISDICTION TO THE FBI[1] A broad, comprehensive list was favored over a more restrictive, narrow one. It is hoped that such an approach will benefit agents working these matters.	
18 U.S.C. §§ 81, 113, 114, 1111, 1112, 1113, 1201, 1363, 2111	CRIMES COMMITTED WITHIN THE SPECIAL MARITIME AND TERRITORIAL JURISDICTION OF THE UNITED STATES
18 U.S.C. §§ 111, 351, 1114, & 1751	CRIMES AGAINST SELECTED UNITED STATES OFFICIALS
18 U.S.C. §§ 112, 878, 1116, & 1201(a)(4)	CRIMES AGAINST INTERNATIONALLY PROTECTED PERSONS
18 U.S.C. § 32	AIRCRAFT SABOTAGE
18 U.S.C. § 33	DESTRUCTION OF MOTOR VEHICLES OR MOTOR VEHICLES FACILITIES
18 U.S.C. § 35	IMPARTING OR CONVEYING FALSE INFORMATION
18 U.S.C. § 37	VIOLENCE AT INTERNATIONAL AIRPORTS
18 U.S.C. § 43	ANIMAL ENTERPRISE TERRORISM
18 U.S.C. § 115	CRIMES AGAINST FAMILY MEMBERS OF A FEDERAL OFFICIAL
18 U.S.C. § 175 - 178	PROHIBITION WITH RESPECT TO BIOLOGICAL WEAPONS
18 U.S.C. § 229 *et seq.*	CHEMICAL WEAPONS
18 U.S.C. §§ 231, 2101[2]	CIVIL DISORDERS; RIOTS
18 U.S.C. § 241[3]	CIVIL RIGHTS CONSPIRACIES
18 U.S.C. § 245[4]	FEDERALLY PROTECTED ACTIVITIES
18 U.S.C. § 247[5]	DAMAGE TO RELIGIOUS PROPERTY
18 U.S.C. § 248[6]	FREEDOM OF ACCESS TO CLINIC ENTRANCES
18 U.S.C. §§ 371, 372	CONSPIRACY
18 U.S.C. § 373	SOLICITATION TO COMMIT A CRIME OF VIOLENCE

[1] The statutes listed are those involving crimes frequently committed by terrorists.

[2] Attorney General approval is required to conduct investigations under these violations, *see* MIOG, Part I, section 157 *et seq.*

[3] Although a violation of this statute is generally investigated as a civil rights crime, if the group committing the offense does so to intimidate or coerce the government or civilian population in furtherance of political or social objectives, the violation may be considered an act of terrorism.

[4] *Id.*

[5] *Id.*

[6] *Id.*

18 U.S.C. § 513	SECURITIES OF THE STATE AND PRIVATE ENTITIES
18 U.S.C. § 514	FICTITIOUS OBLIGATIONS
18 U.S.C. § 641[7]	EMBEZZLE, STEAL, SELL OR CONVERT PUBLIC MONEY, PROPERTY OR RECORDS OF THE UNITED STATES OR ANY DEPARTMENT OR AGENCY
18 U.S.C. § 831	PROHIBITED TRANSACTIONS INVOLVING NUCLEAR MATERIALS
18 U.S.C. § 832[8]	PARTICIPATION IN NUCLEAR AND WEAPONS OF MASS DESTRUCTION THREATS TO THE UNITED STATES
18 U.S.C. § 842(p)	TEACHING, DEMONSTRATING, OR DISTRIBUTION OF INFORMATION RELATIVE TO EXPLOSIVES, DESTRUCTIVE DEVICES AND WEAPONS OF MASS DESTRUCTION
18 U.S.C. § 844[9]	EXPLOSIVE MATERIALS
18 U.S.C. §§ 872 - 880	EXTORTION AND THREATS
18 U.S.C. §§ 921 - 930[10]	UNLAWFUL ACTIVITY: FIREARMS
18 U.S.C. §§ 952 - 970	NEUTRALITY
18 U.S.C. § 1001	FRAUD AND FALSE STATEMENTS
18 U.S.C. § 1014	LOAN AND CREDIT APPLICATIONS GENERALLY; RENEWALS AND DISCOUNTS; CROP INSURANCE
18 U.S.C. § 1028[11]	FRAUD AND RELATED ACTIVITY IN CONNECTION WITH IDENTIFICATION DOCUMENTS AND INFORMATION

[7] *See e.g.,* United States v. Alberico, 604 F.2d 1315 (10th Cir. 1979) (defendant was a United States Army Captain, who stole large quantities of plastic explosives from an Army arsenal, sold them to individuals he believed to be criminals, and would use these explosives in acts of terrorism).

[8] This criminal violation was enacted by the Intelligence Reform And Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[9] Although the FBI has concurrent jurisdiction with the Bureau of Alcohol Tobacco & Firearms and the Postal Inspection Service under this section, by virtue of Jurisdictional Guidelines - published in the United States Attorney's Bulletin on April 13, 1973 for the FBI, ATF, and Postal Inspection Service which became effective March 1, 1973 (commonly referred to as the April 13, 1973 MOU) - the FBI will exercise primary jurisdiction over all alleged violations of section 844 which appear at the outset to have been perpetrated by terrorist/revolutionary groups or individuals. The FBI also is given primary jurisdiction over several other 844 violations even without a terrorism nexus, e.g., offenses involving possession of explosives in buildings owned, leased, used, etc., by the United States; alleged offenses directed against foreign diplomatic facilities; and alleged offenses against colleges and universities.

[10] *See* 20 U.S. Op. OLC 242, Opinion of the Office of Legal Counsel, U.S. Department of Justice, FBI AUTHORITY TO INVESTIGATE VIOLATIONS OF SUBTITLE E OF TITLE 26 OR 18 U.S.C. SECTIONS 921-930, June 21, 1996 (finding where the FBI has a reasonable expectation that if an investigation involves a crime of terrorism over which a statute or Presidential Decision Directive 39 [issued June 21, 1995, but has since been superseded by a National Security Presidential Directive] has granted primary responsibility to the FBI, the FBI's lead role may be extended to cover crimes as to which lead responsibility would otherwise reside elsewhere).

[11] Under the FRAID Statute (18, USC, § 1028), jurisdiction has been divided by the DOJ between the FBI, U.S. Secret Service or the defrauded or investigating Federal agency, if said agency has civilian criminal investigative authority or a Statutory Inspector General, *see* MIOG Part I, sections 253-2.3 & 253-2.4 or MOU between FBI and U.S. Secret Service Pursuant to the Comprehensive Crime Control Act of 1984, dated September 15, 1989.

18 U.S.C. § 1029[12]	FRAUD AND RELATED ACTIVITY IN CONNECTION WITH ACCESS DEVICES
18 U.S.C. § 1030[13]	FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS
18 U.S.C. § 1038[14]	FALSE INFORMATION AND HOAXES
18 U.S.C. § 1074	FLIGHT TO AVOID PROSECUTION FOR DAMAGING OR DESTROYING ANY BUILDING OR OTHER REAL OR PERSONAL PROPERTY
18 U.S.C. § 1091[15]	GENOCIDE
18 U.S.C. § 1117	CONSPIRACY TO MURDER
18 U.S.C. § 1119	FOREIGN MURDER OF UNITED STATES NATIONALS
18 U.S.C. § 1201	KIDNAPPING
18 U.S.C. § 1203[16]	ACT FOR THE PREVENTION AND PUNISHMENT OF THE CRIME OF HOSTAGE TAKING
18 U.S.C. § 1341	MAIL FRAUD
18 U.S.C. § 1343	FRAUD BY WIRE, RADIO, OR TELEVISION
18 U.S.C. § 1344	BANK FRAUD
18 U.S.C. § 1361	GOVERNMENT PROPERTY OR CONTRACTS
18 U.S.C. § 1362	COMMUNICATION LINES, STATIONS OR SYSTEMS
18 U.S.C. § 1363	BUILDINGS OR PROPERTY WITHIN SPECIAL MARITIME AND TERRITORIAL JURISDICTION
18 U.S.C. § 1364	INTERFERENCE WITH FOREIGN COMMERCE BY VIOLENCE
18 U.S.C. § 1365	TAMPERING WITH CONSUMER PRODUCTS
18 U.S.C. § 1366	DESTRUCTION OF AN ENERGY FACILITY
18 U.S.C. § 1367	INTERFERENCE WITH THE OPERATION OF A SATELLITE
18 U.S.C. § 1521	RETALIATING AGAINST A FEDERAL JUDGE OR FEDERAL LAW ENFORCEMENT OFFICER BY FALSE CLAIM OR SLANDER OF TITLE

[12] *See* MOU between FBI and U.S. Secret Service Pursuant to the Comprehensive Crime Control Act of 1984, dated September 15, 1989, or MIOG, Part I, section 258 -1 *et seq.*, for investigative jurisdiction relating to this statute.

[13] *See* MOU between FBI and U.S. Secret Service Pursuant to the Comprehensive Crime Control Act of 1984, dated September 15, 1989, for investigative jurisdiction relating to this statute.

[14] This criminal violation was enacted by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[15] The United States Attorneys' Manual, 9-2.136, Investigative and Prosecutive Policy for International Terrorism Matters (September 1997 Edition), recognizes genocide as an international terrorism offense.

[16] *See also* National Security Presidential Directive - 12, UNITED STATES CITIZENS TAKEN HOSTAGE ABROAD, dated February 18, 2002, which outlines the FBI's responsibilities..

18 U.S.C. §§ 1541 - 1546	CRIMES BASED UPON IMPROPER ACQUISITION OR MISUSES OF PASSPORT, VISA, OR ENTRY DOCUMENTS
18 U.S.C. §§ 1651 - 1661	PIRACY AND PRIVATEERING
18 U.S.C. § 1951	INTERFERENCE WITH COMMERCE BY THREATS OF VIOLENCE
18 U.S.C. § 1952	INTERSTATE AND FOREIGN TRAVEL OR TRANSPORTATION IN AID OF RACKETEERING ENTERPRISES
18 U.S.C. § 1956	MONEY LAUNDERING AS IT RELATES TO TERRORISM OFFENSES
18 U.S.C. § 1957	ENGAGING IN MONETARY TRANSACTIONS IN PROPERTY DERIVED FROM SPECIFIED UNLAWFUL ACTIVITY
18 U.S.C. § 1959	VIOLENT CRIMES IN AID OF RACKETEERING ACTIVITY
18 U.S.C. § 1960	PROHIBITION OF ILLEGAL MONEY TRANSMITTING BUSINESSES
18 U.S.C. § 1962	PROHIBITED ACTIVITIES RELATING TO RICO
18 U.S.C. § 1991	ENTERING TRAIN TO COMMIT A CRIME
18 U.S.C. § 1992	TERRORIST ATTACKS AND OTHER VIOLENCE AGAINST MASS TRANSPORTATION SYSTEMS ON LAND, ON WATER, OR THROUGH THE AIR
18 U.S.C. §§ 2151 et seq.	SABOTAGE
18 U.S.C. § 2237	CRIMINAL SANCTIONS FOR FAILURE TO HEAVE TO, OBSTRUCTION OF BOARDING, OR PROVIDING FALSE INFORMATION
18 U.S.C. § 2261A	INTERSTATE STALKING
18 U.S.C. §§ 2271 - 2282B	DESTRUCTION OF VESSELS; VIOLENCE AGAINST MARITIME NAVIGATION
18 U.S.C. § 2283	TRANSPORTATION OF EXPLOSIVES, BIOLOGICAL, CHEMICAL, OR RADIOACTIVE OR NUCLEAR MATERIALS
18 U.S.C. § 2284	TRANSPORTATION OF TERRORISTS
18 U.S.C. § 2291	DESTRUCTION OF VESSEL OR MARITIME FACILITY
18 U.S.C. § 2292	IMPARTING OR CONVEYING FALSE INFORMATION
18 U.S.C. §§ 2332	TERRORIST ACTS ABROAD AGAINST UNITED STATES NATIONALS
18 U.S.C. § 2332a	USE OF WEAPONS OF MASS DESTRUCTION
18 U.S.C. §, 2332b	ACTS OF TERRORISM TRANSCENDING NATIONAL BOUNDARIES
18 U.S.C. § 2332d[17]	FINANCIAL TRANSACTIONS
18 U.S.C. § 2332f[18]	BOMBINGS OF PLACES OF PUBLIC USE, GOVERNMENT FACILITIES, PUBLIC TRANSPORTATION SYSTEMS AND INFRASTRUCTURE FACILITIES
18 U.S.C. § 2332g[19]	MISSILE SYSTEMS DESIGNED TO DESTROY AIRCRAFT

[17] The FBI has concurrent jurisdiction with the Department of Treasury, and Customs, *see* United States Attorneys' Manual, 9-4.000 - Statutes Assigned by Citation.

[18] See *supra* note 14.

18 U.S.C. § 2332h[20]	RADIOLOGICAL DISPERSAL DEVICES
18 U.S.C. § 2339[21]	HARBORING OR CONCEALING TERRORISTS
18 U.S.C. § 2339A	PROVIDING MATERIAL SUPPORT TO TERRORISTS
18 U.S.C. § 2339B	PROVIDING MATERIAL SUPPORT OR RESOURCES TO DESIGNATED FOREIGN TERRORIST ORGANIZATIONS
18 U.S.C. § 2339C[22]	PROHIBITIONS AGAINST THE FINANCING OF TERRORISM
18 U.S.C. § 2339D[23]	RECEIVING MILITARY TYPE TRAINING FROM A FOREIGN TERRORIST ORGANIZATION
18 U.S.C. § 2340A	TORTURE
18 U.S.C. §§ 2381 et seq.	TREASON, SEDITION, AND SUBVERSIVE ACTIVITIES
18 U.S.C. § 2441	WAR CRIMES
18 U.S.C. § 3286[24]	EXTENSION OF STATUTE OF LIMITATION FOR CERTAIN TERRORISM OFFENSES
21 U.S.C. § 846	ATTEMPT AND CONSPIRACY
21 U.S.C. § 863	DRUG PARAPHERNALIA
21 U.S.C. § 960a	FOREIGN TERRORIST ORGANIZATIONS, TERRORIST PERSONS, AND GROUPS
22 U.S.C. §§ 611 - 621	FOREIGN AGENTS REGISTRATION ACT
22 U.S.C. § 2712[25]	CONTROLS OVER CERTAIN TERRORISM - RELATED SERVICES
22 U.S.C. § 2778	CONTROLS OF ARMS EXPORTS AND IMPORTS (*SEE* 22 C.F.R., PART 127 FOR VIOLATIONS AND PENALTIES)
26 U.S.C. subtit. E, ch. 53[26]	MACHINE GUNS, DESTRUCTIVE DEVICES, AND CERTAIN OTHER FIREARMS

[19]This criminal violation was enacted by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004)

[20] *Id.*

[21] This criminal violation was enacted by the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[22] This criminal violation was enacted by the Suppression of the Financing of Terrorism Convention Implementation Act of 2002, Pub. L. No. 107-197, 116 Stat. 724 (2002).

[23] See *supra* note 18.

[24] As amended by the USA PATRIOT Act, Pub. L. No. 107-56, Title VIII, § 809(a), 115 Stat. 272, 379-380 (2001) (provided no statute of limitation for certain terrorism offenses; and expressly provided that "[t]he amendments made by this section shall apply to the prosecution of any offense committed before, on, or after the date of the enactment of this section [October 26, 2001]."

[25]22, U.S.C. § 2712(f)(2), which pertains to investigations, states, "[t]he Attorney General and the Secretary of Treasury shall have authority to investigate violations of regulations under this section."

[26]See *supra* note 10.

31 U.S.C. § 5332[27]	BULK CASH SMUGGLING INTO OR OUT OF THE UNITED STATES
42 U.S.C. § 2011 - 2284	ATOMIC ENERGY ACT
49 U.S.C. §§ 46501 - 46507	CRIMES ABOARD AN AIRCRAFT; FALSE INFORMATION AND THREATS
49 U.S.C. § 46314	ENTERING AIRCRAFT OR AIRPORT AREA IN VIOLATION OF SECURITY REQUIREMENTS
49 U.S.C. § 60123(b)	DAMAGING OR DESTROYING AN INTERSTATE GAS PIPELINE OR INTERSTATE HAZARDOUS LIQUID PIPELINE FACILITY
49 U.S.C. § 80501	DAMAGE TO TRANSPORTED PROPERTY

OTHER AUTHORITIES RELATING TO THE FBI'S INVESTIGATIVE JURISDICTION IN TERRORISM CASES	
28 U.S.C. § 533	CONFERS ON THE ATTORNEY GENERAL BROAD GENERAL INVESTIGATIVE AUTHORITY WITH RESPECT TO FEDERAL CRIMINAL OFFENSES. UNDER THIS STATUTE, THE ATTORNEY GENERAL "MAY APPOINT OFFICIALS TO DETECT AND PROSECUTE CRIMES AGAINST THE UNITED STATES."
28 U.S.C. § 538	FBI IS AUTHORIZED TO INVESTIGATE ANY VIOLATION OF 49 U.S.C. § 46314 AND VIOLATIONS OF CHAPTER 465 OF TITLE 49 U.S.C. (SPECIAL AIRCRAFT JURISDICTION OF THE UNITED STATES).
5 U.S.C. § 552a(e)(7)	THE FBI SHALL MAINTAIN NO RECORD DESCRIBING HOW ANY INDIVIDUAL EXERCISES RIGHTS GUARANTEED BY THE FIRST AMENDMENT UNLESS EXPRESSLY AUTHORIZED BY STATUTE OR BY THE INDIVIDUAL ABOUT WHOM THE RECORD IS MAINTAINED OR UNLESS PERTINENT TO AND WITHIN THE SCOPE OF AN AUTHORIZED LAW ENFORCEMENT ACTIVITY.
12 U.S.C. § 3414(5)(A)[28]	FINANCIAL INSTITUTIONS SHALL COMPLY WITH FBI REQUEST FOR A CUSTOMER'S OR ENTITY'S FINANCIAL RECORDS.
15 U.S.C. § 1681b(b)(4)	CONDITIONS FOR FURNISHING AND USING CONSUMER REPORTS FOR EMPLOYMENT PURPOSES: EXCEPTION FOR NATIONAL SECURITY INVESTIGATIONS (FAIR CREDIT REPORTING ACT).
15 U.S.C. § 1681u[29]	DISCLOSURE TO FBI FOR COUNTERINTELLIGENCE PURPOSES (FAIR CREDIT REPORTING ACT)

[27] This criminal violation was enacted by the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[28] As amended by the USA PATRIOT Act, Pub. L. No. 107-56, Title III, § 358(f)(2), Title V, § 404, 115 Stat. 272, 327 (2001) (FBI Director or the Director's designee must certify in writing to the financial institution that records sought are for foreign counterintelligence purposes to protect against international terrorism or other clandestine activities). Also, the Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, Title III, Subtitle E, § 374, 117 Stat. 2599, 2628 (2003) significantly expanded the definition of "financial institution" for National Security Letters obtained under the Right to Financial Privacy Act of 1978, e.g., entities now include pawnbrokers, travel agencies, telegraph companies, security dealers and brokers, and commodity futures transactions.

[29] The FBI Director or Director's designee must certify that written request for information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities.

15 U.S.C. § 1681v[30]	DISCLOSURES TO GOVERNMENTAL AGENCIES FOR COUNTERTERRORISM PURPOSES (FAIR CREDIT REPORTING ACT)
26 U.S.C. § 6103(i)(2)	DISCLOSURE OF RETURN INFORMATION OTHER THAN TAXPAYER RETURN INFORMATION FOR USE IN CRIMINAL INVESTIGATIONS
26 U.S.C. § 6103(i)(3)	DISCLOSURE OF RETURN INFORMATION TO APPRISE APPROPRIATE OFFICIALS OF CRIMINAL OR TERRORIST ACTIVITIES OR EMERGENCY CIRCUMSTANCES
26 U.S.C. § 6103(i)(7)	DISCLOSURE UPON REQUEST OF INFORMATION RELATING TO TERRORIST ACTIVITIES
28 U.S.C. § 530C(a)(5)	APPROPRIATIONS RE "ATTORNEY GENERAL EXEMPTION" PROVISION FOR UNDERCOVER OPERATIONS CONDUCTED BY THE FBI[31] October 6, 1992, 106 Stat. 1838, as incorporated by Public Law 104-132, Antiterrorism and Effective Death Penalty Act of 1996, Title VIII, § 815(d), April 24, 1996, 110 Stat. 1315, as amended, which is set out as a note under 28 U.S.C. § 533.
31 U.S.C. § 5318(g)(4)(B)	SECRETARY OF TREASURY'S DESIGNEE SHALL REFER ANY REPORT OF A SUSPICIOUS TRANSACTION TO ANY APPROPRIATE LAW ENFORCEMENT, SUPERVISORY AGENCY, OR UNITED STATES INTELLIGENCE AGENCY FOR USE IN THE CONDUCT OF INTELLIGENCE OR COUNTERINTELLIGENCE ACTIVITIES, INCLUDING ANALYSIS, TO PROTECT AGAINST INTERNATIONAL TERRORISM.
42 U.S.C. § 5197g	FBI IS AUTHORIZED TO INVESTIGATE ESPIONAGE, SABOTAGE, AND SUBVERSIVE ACTS PURSUANT TO TITLE 49, U.S.C., CHAPTER 68 (DISASTER RELIEF), SUBCHAPTER IV-B (EMERGENCY PREPAREDNESS).
50 U.S.C. § 402a[32]	THE FBI MAY INVESTIGATE TO DETERMINE THE SOURCE OF AN UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION AFTER CONSULTING WITH THE EXECUTIVE DEPARTMENT OR AGENCY INVOLVED.
50 U.S.C. § 403-5a[33]	ASSISTANCE TO UNITED STATES LAW ENFORCEMENT AGENCIES

[30] As amended by the USA PATRIOT Act, Pub. L. No. 107-56, Title III, § 358(g)(1)(B), 115 Stat. 272, 327-328 (2001).

[31] The "Attorney General exemption" in subsection (a)(5), means section 102(b) of Public Law 102-395, Department of Justice and Related Agencies Appropriations Act,

[32] This statute requires that the head of each department or agency within the executive branch to advise the FBI immediately of any information which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign agent or an agent of a foreign power.

[33] Elements of the intelligence community may, upon request of a United States law enforcement agency, collect information outside the United States about individuals who are not United States persons. Such elements may collect such information notwithstanding that law enforcement agency intends to use the information collected for purposes of a law enforcement or counterintelligence investigation. Authority for DoD assistance is restricted to (1) the National Security Agency; (2) the National Reconnaissance Office; (3) the National Imagery and Mapping Agency; and (4) the Defense Intelligence Agency. Assistance provided under this section by elements of DoD may not include direct participation of a member of the Army, Navy, Air Force, or Marine Corps in an arrest or similar activity.

50 U.S.C. § 436[34]	REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES FOR FINANCIAL RECORDS OR CONSUMER REPORTS
50 U.S.C. § 1802	AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES
50 U.S.C. § 1822	AUTHORIZATION OF PHYSICAL SEARCHES FOR FOREIGN INTELLIGENCE PURPOSES. *SEE ALSO* EXECUTIVE ORDER 12949, DATED FEBRUARY 9, 1995.
50 U.S.C. § 1842	INSTALLATION AND USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES FOR **FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS**: BASED ON ATTORNEY GENERAL APPROVAL OR DESIGNATED ATTORNEY FOR THE GOVERNMENT FOR FBI TO CONDUCT INVESTIGATIONS UNDER SUCH GUIDELINES AS THE AG APPROVES PURSUANT TO EXECUTIVE ORDER 12333, OR A SUCCESSOR ORDER.
50 U.S.C. § 1861	ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES
50 U.S.C. § 1881a	PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS
50 U.S.C. § 1881b	CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES
50 U.S.C. § 1881c	OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES
50 U.S.C. § 1881d	JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS
10 U.S.C. § 371 note	MILITARY JOINT TASK FORCES HAVE AUTHORITY TO PROVIDE SUPPORT TO LAW ENFORCEMENT AGENCIES CONDUCTING COUNTER-TERRORISM ACTIVITIES
10 U.S.C. § 382[35]	EMERGENCY SITUATIONS INVOLVING CHEMICAL OR BIOLOGICAL WEAPONS OF MASS DESTRUCTION (MILITARY ASSISTANCE)
10 U.S.C. § 2564[36]	PROVISION OF SUPPORT FOR CERTAIN SPORTING EVENTS (MILITARY ASSISTANCE)

[34] Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination.

[35] This statute provides that "[t]he Secretary of Defense, upon request of the Attorney General, may provide assistance in support of Department of Justice activities relating to the enforcement of section 175 [biological weapons] and [229 et seq., chemical weapons] of title 18 during an emergency situation involving a biological or chemical weapon of mass destruction."

[36] This statute provides that "[a]t the request of a Federal, State, or local government agency responsible for providing law enforcement services, security services, or safety services, the Secretary of Defense or the commander of a military installation or other facility of the Department of Defense or the commander of a specified or unified combatant command to provide assistance for the World Cup Soccer Games, the Goodwill Games, the Olympics, and any other civilian sporting event in support of essential security and safety at such event, but only if the Attorney General certifies that such assistance is necessary to meet essential security and safety needs." *See also* MOU Between the Department of Justice and the Department of Defense Concerning Support for Security for Civilian Sporting Events (dated February 10, 1998), and DoD Directive 2000.15, "Support to Special Events," dated November 21, 1994.

32 C.F.R. § 623.2(6)	LOAN POLICIES OF THE ARMY RELATING TO REQUESTS BY FBI DIRECTOR OR SENIOR FBI OFFICIAL FOR MILITARY RESOURCES NEEDED FOR TERRORISM RELATED MATTERS
18 U.S.C. §§ 175a, 229E, 831(d) & (e)(1) & 2332e	REQUESTS FOR MILITARY ASSISTANCE TO ENFORCE PROHIBITION IN CERTAIN EMERGENCIES
18 U.S.C. § 981(a)(1)(G) & (H)[37]	CIVIL FORFEITURE
28 C.F.R. § 8.2[38]	DESIGNATION OF FBI OFFICIALS HAVING SEIZURE AUTHORITY IN FORFEITURE MATTERS
18 U.S.C. § 2516	AUTHORIZATION (BY ATTORNEY GENERAL OR DESIGNATED DOJ OFFICIAL) FOR FBI INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS THAT MAY PROVIDE OR HAS PROVIDED EVIDENCE OF VIOLATIONS OF **E.G., SECTION 175 (RELATING TO BIOLOGICAL WEAPONS); SECTION 229 (RELATING TO CHEMICAL WEAPONS); OR SECTIONS 2332, 2332a, 2332b, 2332f, 2339A, 2339B, or 2339C of TITLE 18 (RELATING TO TERRORISM)**
18 U.S.C. § 2709	COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS THAT ARE "RELEVANT TO AN AUTHORIZED INVESTIGATION TO PROTECT AGAINST INTERNATIONAL TERRORISM OR CLANDESTINE INTELLIGENCE ACTIVITIES."
20 U.S.C. § 1232g	DISCLOSURE OF EDUCATIONAL RECORDS RELATING TO INVESTIGATION AND PROSECUTION OF TERRORISM ("BUCKLEY AMENDMENT")
28 C.F.R. § 0.85	UNDER THIS REGULATION, THE ATTORNEY GENERAL HAS DELEGATED INVESTIGATIVE AUTHORITY TO THE FBI FOR ALL CRIMES NOT OTHERWISE ASSIGNED BY CONGRESS TO ANOTHER AGENCY. IT ALSO PROVIDES THAT THE FBI SHOULD "EXERCISE LEAD AGENCY RESPONSIBILITIES IN INVESTIGATING ALL CRIMES FOR WHICH IT HAS PRIMARY OR CONCURRENT JURISDICTION AND WHICH INVOLVE TERRORIST ACTIVITIES WITHIN THE STATUTORY JURISDICTION OF THE UNITED STATES."
28 C.F.R. § 0.89	THE FBI DIRECTOR IS AUTHORIZED TO EXERCISE AUTHORITY RELATING TO THE SEIZURE OF ARMS AND MUNITIONS OF WAR, AND OTHER ARTICLES AS WELL AS SEIZING AND DETAINING ANY VESSEL, VEHICLE, OR AIRCRAFT CONTAINING SUCH ITEMS PURSUANT TO 22 U.S.C. § 401 (ILLEGAL EXPORTATION OF WAR MATERIALS).

[37] These statutory sections provide civil forfeiture authority relevant to acts of domestic or international terrorism.

[38] The FBI is authorized to seize property subject to seizure pursuant to statutes identified in § 8.1, e.g. 22 U.S.C. § 401, Illegal Exportation of War Materials.

31 C.F.R. § 103.100[39]	INFORMATION SHARING BETWEEN FEDERAL LAW ENFORCEMENT AGENCIES AND FINANCIAL INSTITUTIONS A FEDERAL LAW ENFORCEMENT AGENCY INVESTIGATING TERRORIST ACTIVITY OR MONEY LAUNDERING MAY REQUEST THAT FinCEN SOLICIT, ON THE INVESTIGATING AGENCY'S BEHALF, CERTAIN INFORMATION FROM A FINANCIAL INSTITUTION OR A GROUP OF FINANCIAL INSTITUTIONS BASED ON CREDIBLE EVIDENCE CONCERNING TERRORIST ACTIVITY OR MONEY LAUNDERING.
33 C.F.R. § 233.3	CHIEF POSTAL INSPECTOR OF US POSTAL SERVICE MAY ORDER A MAIL COVER UPON WRITTEN REQUEST FROM THE HEAD OF A LAW ENFORCEMENT AGENCY SPECIFYING REASONABLE GROUNDS THAT DEMONSTRATE THE MAIL COVER IS NECESSARY TO "PROTECT THE NATIONAL SECURITY OF THE UNITED STATES" (E.G., ACTUAL OR POTENTIAL THREATS TO OUR SECURITY; AN ATTACK OR OTHER GRAVE HOSTILE ACT; SABOTAGE OR INTERNATIONAL TERRORISM; AND CLANDESTINE INTELLIGENCE ACTIVITIES).
45 C.F.R. § 164.512(k)(2)	USES AND DISCLOSURES OF HEALTH INFORMATION FOR SPECIALIZED GOVERNMENT FUNCTIONS, NATIONAL SECURITY AND INTELLIGENCE ACTIVITIES: *AUTHORIZING STATUTE TITLE 42, U.S.C., § 1320d-2 NOTE*
DEPARTMENT OF JUSTICE ORDER 1900.5B[40] (3) Responding to specific requests from senior government officials and agencies for FBI information related to foreign counterintelligence and domestic security matters.	NATIONAL SECURITY EMERGENCY PREPAREDNESS PROGRAM AND RESPONSIBILITIES (SEPTEMBER 12, 2003). THE FBI'S RESPONSIBILITIES ARE LISTED IN THIS ORDER

[39] *See* Title 31, U.S.C., § 5311 note, pursuant to USA PATRIOT Act, October 26, 2001, the Secretary of Treasury is required to "adopt regulations to encourage further cooperation among financial institutions, their regulatory authorities, and law enforcement authorities, with the specific purpose of encouraging regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in, or reasonably suspected based on credible evidence of engaging in, terrorist acts or money laundering activities."

[40] According to this Order, the FBI is responsible for providing a response to foreign counterintelligence and domestic security and terrorism threats. This includes:

(1) Directing and coordinating, as circumstances allow, urgent and expanded efforts required by Congressional enactments and executive branch directives to detect and deter hostile activities directed against the United States by foreign or domestic elements;

(2) Disseminating information, to the extent that conditions permit, concerning hostile intentions and activities toward government officials and agencies; and

ATTORNEY GENERAL ORDER NO. 2954-2008[41]	DELEGATION TO THE DIRECTOR OF THE FBI CERTAIN AUTHORITY RELATING TO THE PROVISION OF TECHNICAL ASSISTANCE TO FEDERAL, STATE, LOCAL, AND FOREIGN LAW ENFORCEMENT AGENCIES
ATTORNEY GENERAL ORDER NO. 2857-2007	DELEGATION TO THE DIRECTOR OF THE FBI OF AUTHORITY TO GRANT REWARDS FOR INFORMATION CONCERNING TERRORIST ACTS (18 U.S.C. §§ 3071-77). THE FBI DIRECTOR IS ALSO AUTHORIZED TO DELEGATE THE AUTHORITY TO APPROPRIATE FBI OFFICIALS.
ATTORNEY GENERAL ORDER NO. 2737-2004	DELEGATION OF AUTHORITY TO AUGMENT THE FBI'S JOINT TERRORISM TASK FORCES[42]
ATTORNEY GENERAL ORDER NO. 2654-2003	DELEGATION OF AUTHORITY TO CONDUCT SECURITY CHECKS AND TO TAKE OTHER ACTIONS PURSUANT TO THE PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002[43](specific sections codified at 42 U.S.C. § 262a, 7 U.S.C. § 8401, and 7 U.S.C. § 8411), to receive names and other identifying information submitted by individuals requesting access to specified agents or toxins; utilize electronic databases and other sources of information to conduct background checks and security risk assessments of such individuals; and consult with appropriate officials of the Department of Health and Human Services and the Department of Agriculture as to whether certain individuals specified in the above cited statutory provisions should be denied access to or granted limited access to specified agents.
EXECUTIVE ORDER 12139 (Foreign Intelligence Electronic Surveillance)	PURSUANT TO THE FISA, DIRECTOR AND DEPUTY DIRECTOR OF THE FBI ARE AUTHORIZED TO MAKE THE CERTIFICATIONS REQUIRED BY SECTION 104(a)(6) OF THE ACT IN SUPPORT OF APPLICATIONS TO CONDUCT ELECTRONIC SURVEILLANCE
EXECUTIVE ORDER 12949 (Foreign Intelligence Physical Searches)	PURSUANT TO THE FISA, DIRECTOR AND DEPUTY DIRECTOR OF THE FBI ARE AUTHORIZED TO MAKE THE CERTIFICATIONS REQUIRED BY SECTION 303(a)(6) OF THE ACT IN SUPPORT OF APPLICATIONS TO CONDUCT PHYSICAL SEARCHES

[41]This order sets forth, that, the Director of the FBI is delegated the authority to provide reasonable assistance to foreign national security agencies cooperating with the FBI in the execution of the FBI's counter-terrorism and counter-intelligence duties, and federal, state, local or foreign law enforcement agencies, to assist any such agency in the lawful execution of any authorized function.

[42] This Order provides that pursuant to Attorney General procedures which will be put into place when necessary to prevent or respond to terrorist attacks, the JTTFs can call upon all Department law enforcement resources for assistance, including agents and other resources of the FBI, DEA, ATF, and USMS. The Director of the FBI and the FBI Special Agents in Charge (SAC) or Assistant Directors in Charge (ADIC) serve as heads of the JTTFs.

[43]This Order delegates to the FBI Director the Attorney General's authority and responsibilities under sections 201, 212, and 221 of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188, 116 Stat. 594 (2002)

EXECUTIVE ORDER 12333 as amended (United States Intelligence Activities)[44] Additionally, Title 50, USC, § 401a, defines "counterintelligence" as "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf or foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."	**SECTION 1.3(b)(20)(A) - DIRECTOR OF NATIONAL INTELLIGENCE** THIS SUBSECTION STATES THE DIRECTOR OF THE FBI SHALL COORDINATE CLANDESTINE COLLECTION OF FOREIGN INTELLIGENCE COLLECTED THROUGH HUMAN SOURCES OR THROUGH HUMAN-ENABLED MEANS AND COUNTERINTELLIGENCE ACTIVITIES INSIDE THE UNITED STATES **SECTION 1.7(g) - INTELLIGENCE COMMUNITY ELEMENTS, FBI** THIS SUBSECTION AUTHORIZES THE INTELLIGENCE ELEMENTS OF THE FBI TO (1) COLLECT (INCLUDING THROUGH CLANDESTINE MEANS), ANALYZE, PRODUCE, AND DISSEMINATE FOREIGN INTELLIGENCE AND COUNTERINTELLIGENCE TO SUPPORT NATIONAL AND DEPARTMENTAL MISSIONS; (2) CONDUCT COUNTERINTELLIGENCE ACTIVITIES; AND (3) CONDUCT FOREIGN INTELLIGENCE AND COUNTERINTELLIGENCE LIAISON RELATIONSHIPS WITH INTELLIGENCE, SECURITY, AND LAW ENFORCEMENT SERVICES OF FOREIGN GOVERNMENTS OR INTERNATIONAL ORGANIZATIONS. **SECTION 1.13, THE FBI** - AUTHORIZES THE DIRECTOR OF THE FBI TO PROVIDE TECHNICAL ASSISTANCE, WITHIN OR OUTSIDE THE UNITED STATES, TO FOREIGN INTELLIGENCE AND LAW ENFORCEMENT SERVICES.
EXECUTIVE ORDER 12656 (ASSIGNMENT OF EMERGENCY PREPAREDNESS RESPONSIBILITIES)	AMONG ITS LEAD AGENCY RESPONSIBILITIES, DOJ SHALL COORDINATE FEDERAL GOVERNMENT DOMESTIC LAW ENFORCEMENT ACTIVITIES RELATED TO NATIONAL SECURITY EMERGENCY PREPAREDNESS
EXECUTIVE ORDER 12947 (PROHIBITED TRANSACTIONS WITH TERRORISTS WHO THREATEN TO DISRUPT THE MIDDLE EAST PEACE PROCESS)	ANY INVESTIGATION EMANATING FROM A POSSIBLE VIOLATION OF THIS ORDER MUST BE COORDINATED WITH THE FBI, AND ANY MATTER INVOLVING EVIDENCE OF A CRIMINAL VIOLATION SHOULD BE REFERRED TO THE FBI.
EXECUTIVE ORDER 13128 (IMPLEMENTATION OF THE CHEMICAL WEAPONS CONVENTION AND THE CHEMICAL WEAPONS CONVENTION IMPLEMENTATION ACT)[45]	ANY INVESTIGATION EMANATING FROM A POSSIBLE VIOLATION OF THIS ORDER INVOLVING OR REVEALING A POSSIBLE VIOLATION OF 18, U.S.C., § 229 SHALL BE REFERRED TO THE FBI.

[44]Title 50, USC, § 401a, defines "foreign intelligence" as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."

[45]*See generally,* Title 22, USC, § 6711 (Designation of United States National Authority Pursuant to the Chemical Weapons Convention).

EXECUTIVE ORDER 13388 (FURTHER STRENGTHENING THE SHARING OF TERRORISM INFORMATION)[46]	STATES THAT THE HEAD OF EACH AGENCY THAT POSSESSES OR ACQUIRES TERRORISM INFORMATION SHALL PROMPTLY GIVE ACCESS TO THE TERRORISM INFORMATION TO THE HEAD OF EACH OTHER AGENCY THAT HAS COUNTERTERRORISM FUNCTIONS.
EXECUTIVE ORDER 13491 (ENSURING LAWFUL INTERROGATIONS)	SECTION 3, "STANDARDS AND PRACTICE FOR INTERROGATION OF INDIVIDUALS IN THE CUSTODY OR CONTROL OF THE UNITED STATES IN ARMED CONFLICTS" **(b)** INTERROGATION TECHNIQUES AND INTERROGATION-RELATED TREATMENT[47] *See* H.R. Rep. No. 111-89, 111th Cong., 1st Sess. 2009, "Resolution of Inquiry Requesting that the President and Directing that the Attorney General Transmit to the House of Representatives All Information in Their Possession Relating to Specific Communications Regarding Detainees and Foreign Persons Suspected of Terrorism," June 26, 2009.

[46]Note that this EO refers to section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 for the definition of "terrorism information." This section of the Act is codified in Title 6, USC, section 485, Information sharing.

[47]Section 3(b) of this EO states that nothing in this section shall preclude the FBI, or other Federal law enforcement agencies, from continuing to use authorized, non-coercive techniques of interrogation that are designed to elicit voluntary statements and do not involve the use of force, threats, or promises.

Note that the Detainee Treatment Act of 2005, Pub. L. 109-148, Div. A, Title X, § 1004, Dec. 30, 2005, 119 Stat. 2740, codified at Title 42 U.S.C. § 2000dd-1(a) (Protection of United States Government personnel Engaged in Authorized Interrogations) provides that:

in any civil or criminal prosecution against an officer, employee, member of the Armed Forces, or other agent of the United States Government who is a United States person, arising out of the officer, employee, member of the Armed Forces, or other agent's engaging in specific operational practices, that involve detention and interrogation of aliens who the President or his designees have determined are believed to be engaged in or associated with international terrorist activity that poses a serious threat to the United States, its interests, or its allies, and that were officially authorized and determined to be lawful at the time that they were conducted, **it shall be a defense that such officer, employee, member of the Armed Forces, or other agent did not know that the practices were unlawful.**

Also note that the National Defense Authorization Act for Fiscal Year 2010, Pub. L. 111-84, Title X, § 1040 (No Miranda Warnings for Al Qaeda Terrorists), October 28, 2009, 123 Stat. 2190, 2454, codified at Title 10 U.S.C. § 801 note, provides that:

Absent a court order requiring the reading of such statements, no member of the Armed Forces and no official of the Department of Defense or component of the intelligence community (other than the Department of Justice) may read to a foreign national who is captured or detained outside the United States as an enemy belligerent and is in the custody or under the effective control of the Department of Defense or otherwise under detention in a Department of Defense facility the statement required by Miranda v. Arizona (384 U.S. 436 (1966)), or otherwise inform such an individual of any rights that the individual may or may not have to counsel or remain silent consistent with Miranda v. Arizona (384 U.S. 436 (1966)).

Regarding the practice of Mirandizing terrorist suspects overseas, in a June 12, 2009 letter from FBI Director Robert Mueller to U.S. Congressman Frank Wolf, Director Mueller confirmed that "there has been no policy change and no blanket instruction issued for FBI agents to Mirandize detainees overseas." Furthermore, the Director noted in his letter, that FBI agents have occasionally given Miranda warnings to persons captured overseas, at Bagram Air Base (Afghanistan) and elsewhere, but only when "a determination was made that a prosecution in an Article III court may be in the interest of national security and that providing Miranda warnings . . . was . . . desirable to maximize the likelihood that any resulting statements would be admissible at trial."

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE (NSPD) - 12	ASSIGNS THE FBI LEAD AGENCY RESPONSIBILITIES RELATING TO UNITED STATES CITIZENS TAKEN HOSTAGE ABROAD.
NSPD 28	ADDRESSES FBI'S PRIMARY RESPONSIBILITY CONCERNING UNITED STATES NUCLEAR WEAPONS COMMAND AND CONTROL, SAFETY, AND SECURITY.
NSPD 46/HSPD-15 ANNEX II[48] Additionally, *see e.g.,* Department of Justice, Office of Legal Counsel opinion, FBI AUTHORITY TO INVESTIGATE VIOLATIONS OF SUBTITLE E OF TITLE 26 OR 18 U.S.C. SECTIONS 921-930, June 21, 1996 (the FBI has lead investigative responsibility over crimes of terrorism pursuant to statutes or Presidential Decision Directive 39 that have granted authority to the FBI in these matters). Note that PDD 39 was superseded by a National Security Presidential Directive.	OUTLINES THE FBI'S LEAD JURISDICTIONAL RESPONSIBILITIES IN RELATION TO TERRORISM.
MARITIME STRATEGY FOR MARITIME SECURITY: MARITIME OPERATIONAL THREAT RESPONSE (MOTR)	THE DEPARTMENT OF JUSTICE, ACTING THROUGH THE FBI, IS THE LEAD MOTR AGENCY FOR INVESTIGATIONS OF TERRORIST ACTS OR TERRORIST THREATS BY INDIVIDUALS OR GROUPS INSIDE THE UNITED STATES, OR DIRECTED AT U.S. CITIZENS OR INSTITUTIONS ABROAD, WHERE SUCH ACTS ARE WITHIN THE FEDERAL JURISDICTION OF THE U.S. THE DEPARTMENT OF JUSTICE, ACTING THROUGH THE FBI, IS THE LEAD MOTR AGENCY FOR INTELLIGENCE COLLECTION IN THE UNITED STATES.

[48]By way of historical background, National Security Decision Directive Number 30, MANAGING TERRORIST INCIDENTS, dated April 10, 1982, and National Security Decision Directive Number 207, THE NATIONAL PROGRAM FOR COMBATTING TERRORISM, dated January 20, 1986, were the first Presidential national security directives to grant the FBI lead agency authority to investigate terrorism matters.

As the lead agency to investigate terrorism incidents, the FBI also has authority to investigate terrorism incidents on US Capitol grounds. *See* Department of Justice, Office of Legal Counsel Memorandum for Theodore M. Cooperstein, Counsel to the Deputy Attorney General *Re: FBI Investigative Jurisdiction*, dated June 7, 2004.

DHS, SMALL VESSEL SECURITY STRATEGY, APRIL 2008, APPENDIX A - U.S. FEDERAL GOVERNMENT RESPONSIBILITIES	THE DEPARTMENT OF JUSTICE, ACTING THROUGH THE FBI, IS THE LEAD MOTR AGENCY FOR INVESTIGATIONS OF TERRORIST ACTS OR TERRORIST THREATS BY INDIVIDUALS OR GROUPS INSIDE THE UNITED STATES, OR DIRECTED AT U.S. CITIZENS OR INSTITUTIONS ABROAD, WHERE SUCH ACTS ARE WITHIN THE FEDERAL JURISDICTION OF THE U.S. THE DEPARTMENT OF JUSTICE, ACTING THROUGH THE FBI, IS THE LEAD MOTR AGENCY FOR INTELLIGENCE COLLECTION IN THE UNITED STATES.
NATIONAL STRATEGY FOR AVIATION SECURITY	THE ATTORNEY GENERAL, ACTING THRU THE FBI, IS RESPONSIBLE FOR: (1) INVESTIGATING TERRORIST ACTS OR TERRORIST THREATS BY INDIVIDUALS OR GROUPS INSIDE THE UNITED STATES, OR DIRECTED AT U.S. CITIZENS OR INSTITUTIONS ABROAD; AND (2) INVESTIGATE CRIMINAL VIOLATIONS WITHIN ITS JURISDICTION THAT OCCUR IN THE AIR DOMAIN.
THE NATIONAL STRATEGY TO SECURE CYBERSPACE	THE FBI HAS THE LEAD ROLE TO INVESTIGATE CYBERCRIME
NATIONAL RESPONSE FRAMEWORK (U.S. DEPARTMENT OF HOMELAND SECURITY)	THE NRF IS A GUIDE TO HOW THE NATION CONDUCTS ALL-HAZARDS RESPONSE. **CHAPTER 1: ROLES AND RESPONSIBILITIES, LAW ENFORCEMENT:** - THE ATTORNEY GENERAL, ACTING THROUGH THE FBI, HAS THE LEAD RESPONSIBILITY FOR (1) CRIMINAL INVESTIGATIONS OF TERRORIST ACTS OR TERRORIST THREATS BY INDIVIDUALS OR GROUPS INSIDE THE UNITED STATES OR DIRECTED AT U.S. CITIZENS OR INSTITUTIONS ABROAD; AND (2) COORDINATING ACTIVITIES OF THE OTHER MEMBERS OF THE LAW ENFORCEMENT COMMUNITY TO DETECT, PREVENT, AND DISRUPT TERRORIST ATTACKS AGAINST THE UNITED STATES.
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD) 5	SECRETARY OF HOMELAND SECURITY IS THE PRINCIPAL FEDERAL OFFICIAL FOR COORDINATING DOMESTIC INCIDENT MANAGEMENT. THE ATTORNEY GENERAL HAS LEAD RESPONSIBILITY FOR CRIMINAL INVESTIGATIONS OF TERRORIST ACTS OR THREATS BY INDIVIDUALS OR GROUPS INSIDE THE UNITED STATES, OR DIRECTED AT U.S. CITIZENS OR INSTITUTIONS ABROAD. THE FBI HAS LEAD ROLE FOR COORDINATING THE ACTIVITIES OF OTHER MEMBERS OF THE LAW ENFORCEMENT COMMUNITY TO DETECT, PREVENT, PREEMPT, AND DISRUPT TERRORIST ATTACKS AGAINST THE UNITED STATES. ***ANNEX II TO NSPD-46/HSPD-15 (U.S. POLICY AND STRATEGY IN THE WAR ON TERROR) CLARIFIES THE FBI ROLES AND RESPONSIBILITIES.*
HSPD 7[49]	FBI RESPONSIBLE FOR REDUCING DOMESTIC TERRORIST THREATS, AND INVESTIGATING ACTUAL OR ATTEMPTED TERRORIST ATTACKS OF CRITICAL INFRASTRUCTURE AND KEY RESOURCES.

[49]This Directive supersedes Presidential Decision Directive/NSC-63 of May 22, 1998 ("Critical Infrastructure"), and any Presidential directives issued prior to this directive to the extent of any inconsistency.

ATTORNEY'S GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS	THESE GUIDELINES APPLY TO INVESTIGATIVE ACTIVITIES CONDUCTED BY THE FBI WITHIN THE UNITED STATES OR OUTSIDE THE TERRITORIES OF ALL COUNTRIES. THEY DO NOT APPLY TO INVESTIGATIVE ACTIVITIES OF THE FBI IN FOREIGN COUNTRIES, WHICH ARE GOVERNED BY THE ATTORNEY GENERAL'S GUIDELINES FOR EXTRATERRITORIAL FBI OPERATIONS. **NOTE THESE GUIDELINES WENT INTO EFFECT DECEMBER 1, 2008.
MEMORANDUM OF AGREEMENT BETWEEN THE DOJ AND DHS CONCERNING TERRORIST FINANCING INVESTIGATIONS, SIGNED MAY 13, 2003	DESIGNATES THAT THE FBI WILL LEAD TERRORIST FINANCING INVESTIGATIONS AND OPERATIONS USING NATIONAL JOINT TERRORISM TASK FORCE (NJTTF) AND JOINT TERRORISM TASK FORCES (JTTF).

COMMON FBI ACRONYMS

A/SAC	Acting SAC
A/V	Audio/Video
AA	Ankara
AAG	Assistant Attorney General
AAR	After Action Report
ACD	Automatic Call Distribution
ACS	Automated Case Support
AD	Assistant Director
ADA	Americans with Disabilities Act
ADC	Associate Division Counsel
ADIC	Assistant Director in Charge
ADNET	Antidrug Network
ADP	Automated Data Processing
ADPT	Automated Data Processing and Telecommunications
ADR	Alternative Dispute Resolution
AFB	Air Force Base
AFGE	American Federation of Government Employees
AFID	Alias/False Identification
AFIS	Automated Fingerprint Identification System
AFO	Assault on a Federal Officer
AFOR	Annual Field Office Report
AFOSI	Air Force Office of Special Investigations
AG	Attorney General
AGG	Attorney General Guidelines
AH	Athens
AI	Assistant Inspector or Artificial Intelligence
AIAI	Al-Ittihad al-Islami aka Islamic Union (Somalia)
AID	Agency for International Development
AIIP	Assistant Inspector in Place
AKA	Alias or Also-Known-As
AL	Albany Field Office or Alabama or Annual Leave
ALAT	Assistant Legal Attache

ALF	Animal Liberation Front
ALU	Administrative Law Unit (OGC)
AM	Amman
AN	Anchorage Field Office
ANSIR	Awareness of National Security Issues and Response
AO	Administrative Officer or Auxiliary Office
AOAC	Administrative Officers Advisory Committee
AOB	Average on Board
AOL	America Online (Internet Service Provider)
AOT	Act of Terrorism
AP	Applicant Program

AQ	Albuquerque Field Office
ARC	American Red Cross
ASAC	Assistant Special Agent in Charge
A-SAC	Associate SAC
ASCII	American Standard Code for Information Interchange
ASD	Administrative Services Division
ASG	Abu Sayyat Group (Philippines)
ASOS	Aviation and Surveillance Operations Section (CIRG)
AT	Atlanta Field Office
ATCC	Air Traffic Control Center
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
ATM	Asynchronous Transfer Mode or Automated Teller Machine
AUC	United Self Defense Forces of Colombia/Autodefensas Unidos de Colombia, a foreign terrorist organization
AUSA	Assistant United States Attorney
AVITU	Audio/Video Investigative Technology Unit (ITD)
AVP	Availability Pay
AWOL	Absent Without Official Leave
AY	Almaty

BA	Baltimore Field Office
BATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BAU	Behavioral Analysis Unit (CIRG)
BB	Bridgetown
BC	BICS Administration Group
BD	Budapest ILEA
BDC	Bomb Data Center (LAB)
BE	Buenos Aires
BF	Buffalo Field Office
BG	Bogata
BH	Birmingham Field Office
BI	Brasilia
BIA	Bureau of Indian Affairs (Interior Department)
BICE	Bureau of Immigration and Custom Enforcement
BICS	Background Investigation Contract Service
BK	Bangkok
BL	Brussels
BN	Berlin
BO	Bucharest
BOLO	Be On the Lookout
BOP	Bureau of Prisons
BPMS	Bureau Personnel Management System
BR	Bern
BS	Boston Field Office
BUDED	Bureau Deadline
BW	Biological Warfare
BZ	Beijing
C	Confidential
C/PTDs	Convictions/Pretrial Diversions
CAC	Crimes Against Children
CACU	Crimes Against Children Unit
CAFRA	Civil Asset Forfeiture and Reform Act of 2000
CALEA	Communications Assistance to Law

	Enforcement Act
CAPWIN	Capital Wireless Integrated Network
CART	Computer Analysis and Response Team (ITD)
CASMIRC	Child Abduction and Serial Murder Investigative Resource Center
CAT	Crisis Action Team
CATS	Consolidated Asset Tracking System
CBP	Customs and Border Protection
CBR	Can Be Reached
CBW	Chemical and Biological Warfare
CCP	Cyber Crime Program
CCR	Computerized Criminal Record
CCTV	Closed Circuit TV
CD	Counterintelligence Division or Compact Disc
CDC	Chief Division Counsel or Centers for Disease Control and Prevention
CDL	Commercial Driver's License
CDMA	Code Division Multiple Access (wireless technology standard)
CDPD	Cellular Digital Package Data
CE	Charlotte Field Office or Critical Element
CEAU	Cryptographic and Electronic Analysis Unit (ITD)
CEI	Criminal Enterprise Investigations
CEIP	Criminal Enterprise Investigations Program
CFC	Combined Federal Campaign
CFG	Confidential Funding Guide
CFR	Confidential File Room or Code of Federal Regulations
CG	Chicago Field Office
CGR	Crime on Government Reservations
CH	Copenhagen
CI	Cincinnati Field Office or Confidential Informant
CIA	Central Intelligence Agency
CIC	Counterintelligence Center (CIA)
CID	Criminal Investigative Division (FBI)

CIITAC	Computer Investigations and Infrastructure Threat Assessment Center
CIMS	Criminal Informant Management System
CIO	Chief Information Officer

CIP	Criminal Informant Program
CIPA	Classified Information Protection Act
CIRG	Critical Incident Response Group
CISP	Criminal Intelligence Support Program
CJIS	Criminal Justice Information Services Division
CLEA	Criminal Law Enforcement Application
CLEIG	Combined Law Enforcement Intelligence Group
CMU	Crisis Management Unit (CIRG)
CN	Canberra
CNC	DCI Crime and Narcotics Center
CNN	Cable News Network
CNU	Crisis Negotiations Unit (CIRG)
CO	Columbia Field Office
COB	Close of Business
COBB	Carry Over Briefing Book
COG	Continuity of Government
COL	Color of Law
COMSAT	Communications Satellite
COMSEC	Communications Security
CONOP(S)	Concept of Operation(s)
CONUS	Continental United States
COOP	Continuity of Operations Plan
COP	Chief of Police or Community Outreach Program
COPS	Community Oriented Policing Services (DOJ)
COS	Chief of Station (CIA)
COTR	Contract Officer's Technical Representative
COTS	Commercial off-the-shelf (software)
CP	Command Post
CPU	Central Processing Unit

CR	Caracas or Civil Rights
CRP	Civil Rights Program
CRT	Cathode Ray Tube (Terminal) or Crisis Response Team
CRU	Crisis Response Unit (ITD)
CS	Computer Specialist or Confidential Source
CSRS	Civil Service Retirement System
CT	Counterterrorism
CTAWU	Counterterrorism Threat Assessment and Warning Unit
CTC	Counter Terrorist Center (CIA)
CTD	Counterterrorism Division (FBI)
CTI	Computer Telephony Integration
CTS	Cyber Technology Section (ITD)
CV	Cleveland Field Office
CW	Chemical Warfare or Cooperative Witness
CYD	Cybercrime Division
CZ	Cairo

D1	Division One - CJIS
D10	Inspection Division (INSD)
D11	Security Division
D12	Finance Division (FD)
D13	Counterterrorism Division (CTD)
D14	Investigative Services Division (defunct)
D16	Cybercrime Division (CYD)
D17	Records Management Division (RMD)
D18	Investigative Technology Division (ITD)
D2	Training Division (TD)
D3	Administrative Services Division (ASD)
D4	Information Resources Division (IRD)
D5	Counterintelligence Division (CD)
D6	Criminal Investigative Division (CID)
D7	Laboratory Division (LAB)

D9	Office of the General Counsel (OGC)
DAD	Deputy Assistant Director
DAG	Deputy Attorney General
DAP	Deliberate Assault Plan
DARPA	Defense Advanced Research Projects Agency
DAWY	Direct Agent Workyear
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCIS	Defense Criminal Investigative Service
DD	Deputy Director
DDN	Defense Data Network
DDO	Deputy Director of Operations (CIA)
DE	Detroit Field Office
DEA	Drug Enforcement Administration
DES	Data Encryption Standard
DEST	Domestic Emergency Support Team
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIA	Defense Intelligence Agency
DIDO	Designated Intelligence Disclosure Official
DINSUM	Defense Intelligence Summary
DISA	Defense Information Systems Agency
DISC	Defense Intelligence Summary Cable
DISCO	Defense Industrial Security Contracting Office
DISN	Defense Information Systems Network
DISSEM	Dissemination
DITU	Data Intercept Technology Unit (ITD)
DJ	Security Division
DK	Records Management Division (RMD)

DL	Dallas Field Office

DLA	Defense Logistics Agency
DLAT	Deputy Legal Attache or Defense Language Aptitude Test
DM	Cybercrimes Division (CYD)
DMA	Defense Mapping Agency
DMV	Department of Motor Vehicles
DN	Denver Field Office
DNA	Deoxyribonucleic Acid
DO	Director's Office
DOB	Date of Birth
DOC	Department of Commerce
DOCX	Document Exploitation
DOD	Department of Defense
DOE	Department of Energy
DOEd	Department of Education
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOMTERR	Domestic Terrorism
DOS	Department of State
DOT	Date of Theft or Department of Transportation
DP	Investigative Technology Division (ITD)
DPOB	Date, Place of Birth
DRSN	Defense Red Switch Network
DS&T	Directorate of Science & Technology (CIA)
DSN	Defense Switched Network
DSNET	Defense Integrated Secure Network
DSS	Diplomatic Security Service (USDS) or Defense Security Service (DOD)
DST	Daylight Savings Time
DT	Domestic Terrorism
DTG	Date-Time Group
DTO	Drug Trafficking Organization
DTRA	Defense Threat Reduction Agency
DTSA	Defense Technology Security Administration

E-mail	Electronic mail
EAD	Executive Assistant Director
EAP	Employee Assistance Program or Emergency Assault Plan
EARS	ELSUR Automated Records System
EAS	Emergency Action Specialist
EBR	Executive Briefing Room (SIOC)
EC	Electronic Communication
ECF	Electronic Case File
ECR	Executive Conference Room (SIOC)
EDI	Executive Development Institute
EDSP	Executive Development and Selection Program
EEI	Essential Elements of Information
EEO	Equal Employment Opportunity
EFT	Electronic Funds Transfer
ELF	Earth Liberation Front
ELN	Colombian National Liberation Army
ELSUR	Electronic Surveillance
EM	Executive Management
EO	Executive Order
EOC	Eurasian Organized Crime
EOD	Entry on Duty or Explosive Ordnance Disposal
EOP	Executive Office of the President
EOUSA	Executive Office of U.S. Attorneys (DOJ)
EP	El Paso Field Office
EPA	Environmental Protection Agency
EPIC	El Paso Intelligence Center
ERF	Engineering Research Facility - Quantico
ERL	Electronic Reference Library
ERT	Emergency Response Team
ERTU	Emergency Response Team Unit (LAB)
ET	Electronics Technicians
ETA	Estimated Time of Arrival or Basque Fatherland and Liberty, aka Euzkadi Ta Askatasuna

EU	European Union
EVP	Evidence Program
FA	Financial Analyst or Financial Assistant
FAA	Federal Aviation Administration
FAG	Fraud Against the Government
FAM	Federal Air Marshal
FAMA	Federal Air Marshal Association
FAR	Federal Acquisition Regulations
FARC	Revolutionary Armed Forces of Colombia
FAST	Forfeiture and Asset Seizure Team
FBIHQ	FBI Headquarters
FBIRA	FBI Recreation Association
FBIS	Foreign Broadcast Information Service
FCC	Federal Communications Commission
FCI	Foreign Counterintelligence
FD	Finance Division
FDA	Food and Drug Administration
Fed	Federal Reserve System
FEDS	Front End Distribution System
FEDSIM	Federal Computer Performance Evaluation and Simulation Center
FEGLI	Federal Employees Government Life Insurance
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FERS	Federal Employees Retirement System
FEST	Foreign Emergency Support Team
FGI	Foreign Government Information
FI	Full Investigation
FIF	Financial Institution Fraud
FIS	Foreign Intelligence Service
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance

b7E

	Court
FISUR	Physical Surveillance
FM	Financial Manager
FMU	Facility Management Unit (ASD)
FNU	First Name Unknown
FOIA	Freedom of Information Act
FOIPA	Freedom of Information/Privacy Acts
FOUO	For Official Use Only
FSL	Funded Staffing Level
FTO	Foreign Terrorist Organization
FTS	Federal Telephone System
FTTTF	Foreign Terrorist Tracking Task Force
FTX	Field Training Exercise
FUG	Fugitive
FY	Fiscal Year
FYI	For Your Information
GAO	General Accounting Office
GATT	General Agreement on Tariffs and Trade (UN)
GF	Government Fraud
GIA	Global Index Application
GITMO	USMC Base, Guantanamo Bay, Cuba
GIWG	Global Intelligence Working Group
GMT	Greenwich Mean Time (Zulu)
GOU	Global Operations Unit
GPO	Government Printing Office
GPRA	Government Performance and Results Act
GPS	Global Positioning System
GRC	Government Reservation Crimes
GS	General Schedule
GSA	General Services Administration
HAMAS	Islamic Resistance Movement
HAZMAT	Hazardous Materials
HC	Hate Crime
HCF	Health Care Fraud

HEPA	High Efficiency Particulate Air Filters

HHS	Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HK	Hong Kong
HMRT	Hazardous Materials Response Team
HMRU	Hazardous Materials Response Unit (LAB)
HN	Honolulu Field Office
HO	Houston Field Office
HR	Human Resources
HRMS	Human Resources Management Section
HRT	Hostage Rescue Team
HTML	Hypertext Markup Language
HUD	Housing and Urban Development
HUMINT	Human Resources Intelligence
HZ	Hermosillo, Mexico
IA	Investigative Assistant or Investigative Analyst
IAATI	International Association of Auto Theft Investigators
IACP	International Association of Chiefs of Police
IAD	Dulles International Airport
IAFC	International Association of Fire Chiefs
IAFIS	Integrated Automated Fingerprint Identification System
IB	Intelligence Base
IBIS	Interagency Border Inspection System
IC	Indian Country or Intelligence Community or Internet Cafe
ICBM	Intercontinental Ballistic Missile
ICE	Immigration and Customs Enforcement (DHS)
ICM	Investigative Case Management
I-CON	Information Control
[redacted]	[redacted] b7E
IED	Improvised Explosive Device
IG	Inspector General

IIIA	Integrated Intelligence Information Application
IINI	Innocent Images National Initiative
IIP	Inspector in Place
IIR	Intelligence Information Report
ILEA	International Law Enforcement Academy, Budapest
IM	Instant Messaging
IMA	Information Management Assistant
IMINT	Imagery Intelligence
IN	Interpol
INMARSAT	International Maritime Satellite
INS	Immigration and Naturalization Service
INSD	Inspection Division
INTERPOL	International Criminal Police Organization
INTERR	International Terrorism
INTSUM	Intelligence Summary

IO	Intelligence Officer
IOB	Intelligence Oversight Board
IOS	Intelligence Operations Specialist
IP	Indianapolis Field Office or Internet Protocol
IR	CIRG
IRD	Information Resources Division
IRS	Intelligence Research Specialist or Internal Revenue Service
IS	Islamabad
ISDN	Integrated Services Digital Network - capacity is 128 kbps
ISP	Internet Service Provider
ISRAA	Integrated Statistical Reporting and Analysis Application
IT	Information Technology or Interstate Theft or International Terrorism
ITC	Information Technology Center
ITD	Investigative Technology Division
ITL	Internet Tip Line
ITM	Information Technologies Manager

ITOS	International Terrorism Operations Section
ITSMV	Interstate Transportation of Stolen Motor Vehicles
ITSP	Interstate Transportation of Stolen Property
IVR	Interactive Voice Response
JCS	Joint Chiefs of Staff
JDIG	Joint Drug Intelligence Group
JEH	J. Edgar Hoover Building
JEM	Jaish-e-Mohammed (Army of Mohammed) (Pakistan)
JFK	John F. Kennedy International Airport
JI	Jemaah Islamiya (Southeast Asia)
JK	Jacksonville Field Office
JN	Jackson Field Office
JOC	Joint Operations Center
JSOC	Joint Special Operations Command or Joint Special Operations Center
JTF-6	Joint Task Force-6
JTFTF	Joint Terrorist Financing Task Force
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
KC	Kansas City Field Office
KMA	Retirement-eligible Special Agent
KSA	Knowledge, Skills and Ability
KV	Kiev
KX	Knoxville Field Office
LA	Los Angeles Field Office or Language Analyst
LAB	Laboratory Division
LAN	Local Area Network
LANL	Los Alamos National Laboratory
LCN	La Cosa Nostra
LD	Laboratory Division
LEA	Law Enforcement Agency
Legat	Legal Attache
LEO	Law Enforcement Online

LES	Law Enforcement Services or Law Enforcement Sensitive
LG	Lagos
LHM	Letterhead Memorandum
LLNL	Lawrence Livermore National Laboratory
LNO	Liaison Officer
LNU	Last Name Unknown
LO	Liaison Office(r) or Lookout or Legat London
LR	Little Rock Field Office
LS	Louisville Field Office or Language Specialist
LTTE	Liberation Tigers of Tamil Eelam (Sri Lanka)
LV	Las Vegas Field Office
LWOP	Leave Without Pay
MAOP	Manual of Administrative Operations and Procedures
MC	Moscow
MD	Madrid
ME	Memphis Field Office
MGMT	Management
MH	Manila
MIOG	Manual of Investigative Operations and Guidelines
MLAT	Mutual Legal Assistance Treaty
MLO	Military Liaison Officer
MM	Miami Field Office
MO	Mobile Field Office or Modus Operandi
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Minneapolis Field Office or Military Police
MRTA	Tupac Amaru Revolutionary Movement (Peru)
Msg	Message
MTTCU	Major Theft/Transportation Crimes Unit
MW	Milwaukee Field Office
MX	Mexico City
NA	FBI National Academy

NAACP	National Association for the Advancement of Colored People
NAC	New Agents Class
NALC	National Association of Letter Carriers
NAS	National Alert System
NATA	North Atlantic Treaty Organization
NATO	

NATU	New Agent Training Unit (TD)
NCAVC	National Center for the Analysis of Violent Crime
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NCMEC	National Center for Missing and Exploited Children
NCTC	National Counterterrorism Center
NDIC	National Drug Intelligence Center
NDPO	National Domestic Preparedness Office
NE	Ft. Monmouth ITC
NEOB	New Executive Office Building
NF	No Foreign Dissemination or Norfolk Field Office
NFI	Not Further Identified or No Further Information or National Foreign Intelligence
NFIB	National Foreign Intelligence Board
NFIP	National Foreign Intelligence Program
NGS	National Gang Strategy
NH	New Haven Field Office
NI	Nairobi
NIBIN	National Integrated Ballistic Information Network
NICB	National Insurance Crime Bureau
NICS	National Instant Criminal Background Check System
NIH	National Institutes of Health
NIMA	National Imagery and Mapping Agency
NIPC	National Infrastructure Protection Center
NIPCIP	National Infrastructure Protection and Computer Intrusion Program

NIPRNET	Unclassified But Sensitive Internet Protocol Router Network
NJTTF	National JTTF
NK	Newark Field Office
NL	New Delhi
NLETS	National Law Enforcement Telecommunications System
NMCC	National Military Command Center
NO	New Orleans Field Office
NOC	Negotiations Operations Center or Network Operations Center
NOFORN	Not Releasable to Foreign Nationals
NOIWON	National Operations and Intelligence Watch Officers Network
NORAD	North American Aerospace Defense Command
NORTHCOM	Northern Command, Colorado Springs, CO
NPO	National Press Office, FBIHQ
NPTL	National Priority Target List
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office

NSA	National Security Agency or National Sheriff's Association
NSC	National Security Council
NSLU	National Security Law Unit (OGC)
NSTL	National Security Threat List
NTWS	National Threat Warning System
NVG	Night Vision Goggles
NWS	National Weather Service
NY	New York City Field Office
OADR	Originating Agency's Determination Required
OC/D	Organized Crime/Drug
OC/DP	Organized Crime/Drug Program
OCA	Original Classification Authority or Office of Congressional Affairs
OCDETF	Organized Crime Drug Enforcement Task Force
OCE	Organized Criminal Enterprises

OCIO	Office of Chief Information Officer
OCIS	Organized Crime Information System
OCONUS	Outside CONUS
OCR	Optical Character Reader/Recognition
OEEOA	Office of Equal Employment Opportunity Affairs
OEO	Office of Enforcement Operations (DOJ)
OEOB	Old Executive Office Building
OFAC	Office of Foreign Asset Control (Treas)
OGA	Other Government Agency
OGC	Office of General Counsel
OIA	Office of International Affairs (DOJ)
OIG	Office of Inspector General
OIO	Office of International Operations
OLEC	Office of Law Enforcement Coordination
OM	Omaha Field Office
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OO	Office of Origin
OPA	Office of Public Affairs
OPM	Office of Personnel Management
OPORD	Operations Order
OPR	Office of Professional Responsibility
OPS	Operations
OPSEC	Operational Security
ORCON	Dissemination and Extraction of Information Controlled by Originator or Originator Controlled
OSC	On-Scene Commander
OSHA	Occupational Safety and Health Administration
OSIRIS	Online Searchable Integrated Reference Information System

OT	Overtime
OTU	Operations and Training Unit, CIRG
PA	Paris or Probationary Agent or Program Analyst

PAC	Public Access Center (SIOC)
PAP	Probationary Agent Program
PAR	Performance Appraisal Report
PAS	Performance Appraisal System
PC	Panama City or Public Corruption or Personal Computer
PCOR	Program Coordinator
PD	Portland Field Office or Police Department
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PDF	Portable Document File - viewable with Adobe Acrobat software
PFI	Principal Firearms Instructor
PFLP	Popular Front for the Liberation of Palestine
PG	Pittsburgh Field Office
PH	Philadelphia Field Office
PI	Preliminary Investigation
PIC	Pilots in Command
PIJ	Palestine Islamic Jihad
PIN	Personal Identification Number
PKK	Kurdistan Workers' Party (Turkey)
PLF	Palestine Liberation Front
PLO	Palestine Liberation Organization
PM	Program Manager
PNG	Persona Non Grata
POC	Point of Contact
POE	Point of Entry
POV	Privately Owned Vehicle
PP	Pay Period
PPMS	Procurement and Property Management Section (FD)
PR	Prague
PRAU	Performance Recognition and Awards Unit (PRAU)
PRL	Personnel Resource List
PSOBO	Public Safety Officer's Benefits Office (DOJ)
PSTN	Public Switched Telephone Network

PT	Pretoria or Physical Training
PX	Phoenix Field Office
QSI	Quality Step Increase
RA	Resident Agency
RAC	Resident Agent in Charge
RCMP	Royal Canadian Mounted Police
RDLU	Rapid Deployment and Logistics Unit (CIRG)
RDOC	Rapid Deployment Operations Center (Aquia)

REI	Racketeering Enterprise Investigation
REL	Releasable
RFU	Radical Fundamentalist Unit (CTD)
RH	Richmond Field Office
RICO	Racketeering Influenced and Corrupt Organization
RISS	Regional Information Sharing System
RMA	Resource Management and Allocation
RMAB	Resource Management and Allocation Board
RMD	Records Management Division
RO	Rome
ROM	Read Only Memory
RSIMS	Rapid Start Information Management System
RSO	Regional Security Officer (U.S. Embassy)
RY	Riyadh
S	~~Secret~~
SA	Special Agent or San Antonio Field Office
SAA	Special Agent Accountant
SAAC	Special Agent Advisory Committee
SABT	Special Agent Bomb Technician
SAC	Special Agent in Charge
SACS	Secure Access Control System
SAMBA	Special Agents Mutual Benefits Association
SAMMS	Special Agent Mid-Level Management Selection (System) or (Board)

SAMNET	Secure Automated Message Network
SAR	Suspicious Activity Report
SAS	Supervisory Administrative Specialist
SAUSA	Special Assistant United States Attorney
SBA	Small Business Administration
SC	Sacramento Field Office or Section Chief or South Carolina
SCI	Sensitive Compartmented Information
SCIF	SCI Facility
SCION	Sensitive Compartmented Information Operational Network
SCOPE	Secure Counterterrorism Operational Prototype Environment
SCS	Supervisory Computer Specialist
SD	San Diego Field Office or Security Division
SDNY	Southern District of New York
SE	Seattle Field Office
SEAS	Supervisory EAS
SEATO	Southeast Asia Treaty Organization
SEC	Securities and Exchange Commission
SEMU	Special Events Management Unit (CTD)
SERL	Special Events Readiness Level
SES	Senior Executive Service
SF	San Francisco Field Office
SG	Singapore
SHAC	Stop Huntingdon Animal Cruelty - an animal rights extremist group
SI	Springfield Field Office
SIGINT	Signals Intelligence
SIOC	Strategic Information and Operations Center
SIPRNET	~~Secret~~ Internet Protocol Router Network
SISG	SIOC Information Support Group
SITREP	Situation Report
SIU	Sensitive Investigation Unit
SJ	San Juan Field Office

SL	St. Louis Field Office or Sick Leave or Sendero Luminoso - aka Shining Path (Peru)
SMEAC	Situation, Mission, Execution, Administration, Command & Control
SMR	SIOC Morning Report
SMTP	Single Mail Transfer Protocol
SN	Santiago
SO	Seoul or Sheriff's Office
SOD	Special Operations Division, Drug Section (CID)
SOG	Special Operations Group or Surveillance Observation Group
SOP	Standard Operating Procedure
SRU	Strategic Resources Unit (ITD)
SSA	Supervisory Special Agent
SSAN	Social Security Account Number
SSG	Special Surveillance Group
SSGU	Safe Streets and Gangs Unit (VCMOS, CID)
SSRA	Supervisory Senior Resident Agent
SSS	Support Services Section
SST	Support Services Technician
ST	Santo Domingo or State
STATE	United States Department of State
STE	Secure Telephone Equipment
STU	Secure Telephone Unit
SU	Salt Lake City Field Office
SVTS	Secure Video Teleconferencing System
SWAT	Special Weapons and Tactics
SWB	Southwest Border
SWS	SIOC Watch Supervisor
T&A	Time and Attendance
T1	1.54 Megabits per Second Throughput (Data Line)
T3	44.3 Megabits per Second Throughput (Data Line)
TA	Telephone Application
TACSAT	Tactical Satellite

TB	Butte ITC
TC	Transportation Crimes
TCU	Telecommunications Services Unit (IRD)
TD	Training Division
TDD	Training and Development Division
TDY	Temporary Duty
TE	Tel Aviv
TECS	Treasury Enforcement Communications System
TEI	Terrorist Enterprise Investigation
TFIS	Theft from Interstate Shipment
TFO	Task Force Officer
TFOS	Terrorist Financing Operations Section
TIS	Technical Information Specialist
TL	Tallinn
TM	Telecommunications Manager
TMU	Threat Management Unit (CTD)
TO	Tokyo
TOC	Tactical Operations Center
TOS	Technical Operations Section (ITD)
TP	Tampa Field Office
TREAS	Department of the Treasury
TRRS	Terrorist Reports and Requirements Section
TS	~~Top Secret~~ or Savannah ITC or Telecommunications Specialist
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSL	Targeted Staffing Level
TSP	Thrift Savings Plan
TS/SCI LAN	~~Top Secret~~/Sensitive Compartmented Information local area network
TTA	Technically Trained Agent
TTIC	Terrorist Threat Integration Center
TTX	Table Top Exercise
TTY	Teletype
TU	Transfer Unit (ASD)
TURK	Time Utilization and Record Keeping

TVA	Tennessee Valley Authority
TWWU	Terrorist Watch and Warning Unit
TZ	Tijuana, Mexico
U	Unclassified
UACB	Unless Advised to the Contrary by the Bureau
UAE	United Arab Emirates

UAV	Unmanned Aerial Vehicle
UBLU	Usama bin Laden Unit
UC	Unit Chief
UCA	Undercover Agent
UCFN	Universal Case File Number
UCMJ	Uniform Code of Military Justice
UCO	Undercover Operation
UCR	Uniform Crime Report
UFAP	Unlawful Flight to Avoid Prosecution
UI	Unidentified
UNI	Universal Index
UNSUB	Unknown Subject
UPS	Uninterruptible Power Supply or United Parcel Service
UR	Urgent Report
URL	Uniform Resource Locator
USA	United States of America or United States Attorney or United States Army
USACID	United States Army Criminal Investigative Division
USAF	United States Air Force
USAO	United States Attorney's Office
USBP	United States Border Patrol
USC	United States Code
USCG	United States Coast Guard
USCS	United States Customs Service
USDA	United States Department of Agriculture
USDAO	United States Defense Attache Office
USDC	United States District Court
USDJ	United States District Judge

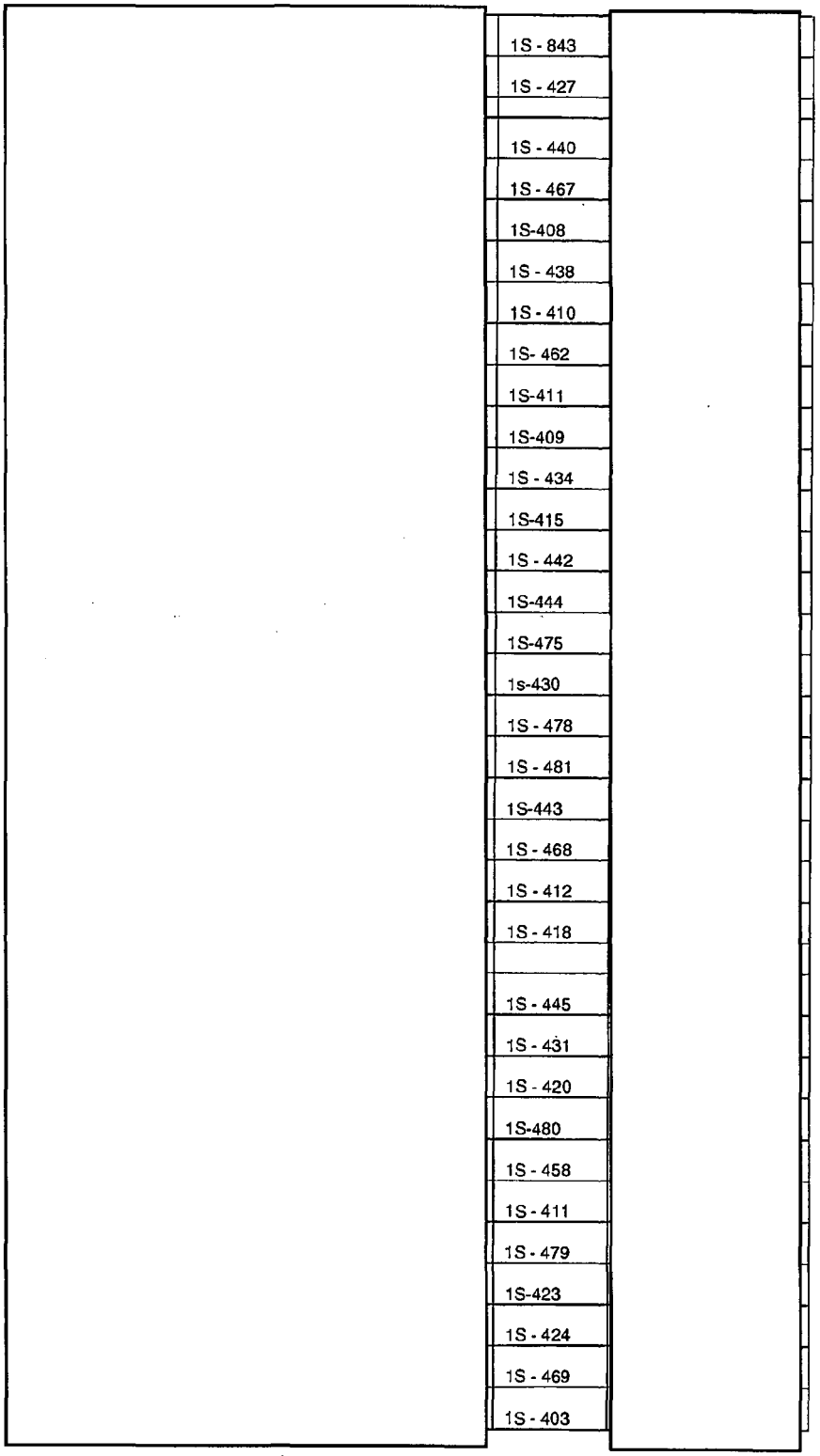
USDS	United States Department of State
USG	United States Government
USIA	United States Information Agency
USIC	United States Intelligence Community
USMC	United States Marine Corps
USMS	United States Marshals Service
USN	United States Navy
USOU	Undercover and Special Operations Unit (CID)
USPER	United States Person
USPIS	United States Postal Inspection Service
USPP	United States Park Police
USPS	United States Postal Service
USSS	United States Secret Service
VA	Veterans Administration
VBIED	Vehicle-Borne Improvised Explosive Device
VCF	Virtual Case File
VCFU	Violent Crimes/Fugitive Unit (CID)
VCMO	Violent Crimes and Major Offenders
VCMOP	Violent Crimes and Major Offenders Program
VCMOS	Violent Crimes and Major Offenders Section (CID)
VCR	Video Cassette Recorder
VCTF	Violent Crimes Task Force
VG	Violent Gangs
VGTOF	Violent Gangs and Terrorist Organizations File
VIC	Violent Incident Crime
VICAP	Violent Criminal Apprehension Program
VIN	Vehicle Identification Number
VIP	Very Important Person
VLTP	Voluntary Leave Transfer Program
VN	Vienna
VPN	Virtual Private Network
VTC	Video Teleconferencing

VWAP	Victim Witness Assistance Program
WAN	Wide Area Network
WCC	White Collar Crime
WCCP	White Collar Crime Program
WE	Pocatello ITC
WF	Washington Field Office
WFO	Washington Field Office
WHCA	White House Communications Agency
WHSR	White House Situation Room
WIGI	Within Grade Increase
WMD	Weapons of Mass Destruction
WMDOU	WMD Operations Unit (CTD)
WR	Warsaw
WSP	Witness Security/Protection
WWW	World Wide Web
X	Exempted from Ten Year Declassification
Z	Zulu Time (Greenwich Mean Time)
ZULU	Greenwich Mean Time

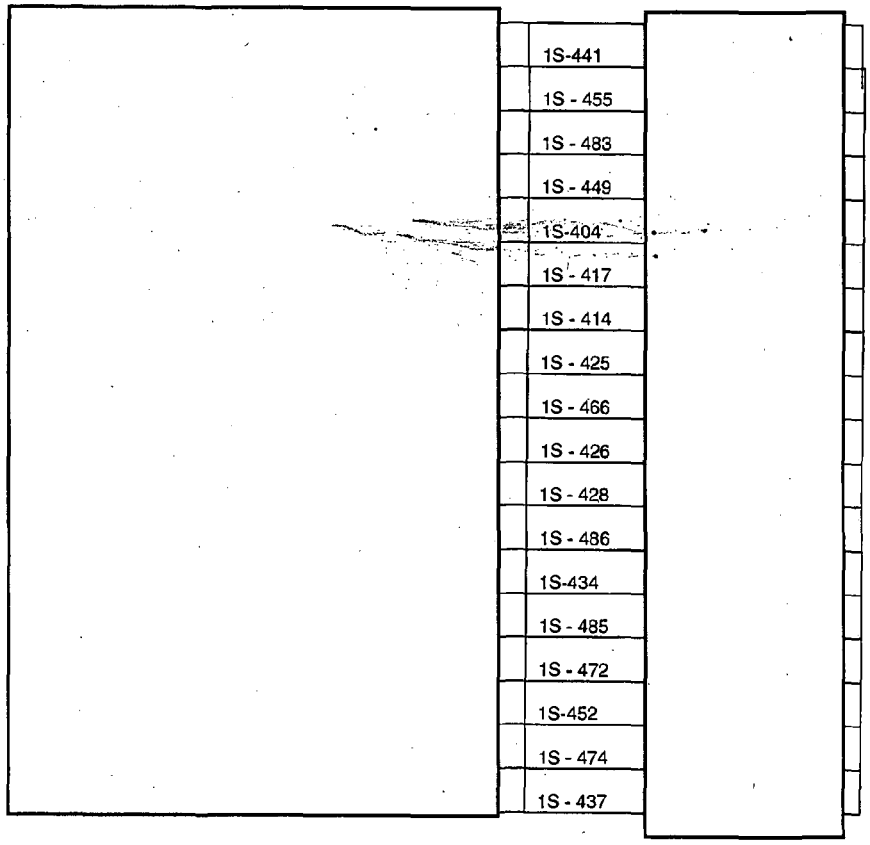
NJTTF MASTER PERSONNEL ROSTER

Official Bureau Name (Last, First, MI)	Agency	Seat Assignment	Secure	NJTTF Office
		1S - 476		
		1S - 435		
		1S-442		
		1S-438		
		1S-408		
		1S - 473		
		1S - 482		
		1S-465		
		1S - 433		
		1S-460		
		1S - 446		
		1S - 489		
		1S - 413		
		1S - 484		
		1S-456		
		1S - 402		
		1S - 430		
		1S-451		
		1S-429		
		1S-461		
		1S-488		
		1S-487		
		1S - 470		
		1S - 471		
		1S - 416		
		1S-477		
		1S - 447		
		1S- 465		
		1S - 448		
		1S-450		

b6
b7C


1S - 843
1S - 427
1S - 440
1S - 467
1S-408
1S - 438
1S - 410
1S- 462
1S-411
1S-409
1S - 434
1S-415
1S - 442
1S-444
1S-475
1s-430
1S - 478
1S - 481
1S-443
1S - 468
1S - 412
1S - 418
1S - 445
1S - 431
1S - 420
1S-480
1S - 458
1S - 411
1S - 479
1S-423
1S - 424
1S - 469
1S - 403

b6
b7C


1S-441
1S - 455
1S - 483
1S - 449
1S-404
1S - 417
1S - 414
1S - 425
1S - 466
1S - 426
1S - 428
1S - 486
1S-434
1S - 485
1S - 472
1S-452
1S - 474
1S - 437

b6
b7C

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/24/2009

To: All Field Offices **Attn:** ADIC/SAC
JTTF/CT ASACs
JTTF/CT SSAs/SSRAs
JTTF Coordinators

Counterterrorism **Attn:** DAD Tracy A. North
DAD Virginia L. Bollinger

From: Counterterrorism
DTRS/National Joint Terrorism Task Force
Contact: IA [redacted]

Approved By: McJunkin, James W
Ward, Michael B
Giuliano, Mark [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: 415A-HQ-C1432188-DR (Pending)

Title: NATIONAL JOINT TERRORISM TASK FORCE;
DATABASE/RESOURCE SUPPORT

Synopsis: To inform Joint Terrorism Task Forces (JTTFs) on the availability of National Joint Terrorism Task Force's (NJTTF) databases and resources.

Administrative: Field JTTF members are encouraged to coordinate with their local JTTF federal, state and local representatives prior to contacting the NJTTF.

Details: The NJTTF's mission is focused on providing support to other Counterterrorism Division Sections and field JTTFs. The NJTTF does this through access to [redacted] available through its [redacted] plus Task Force Officers (TFOs) from federal, state and local government agencies. b7E

Supported units gain unique assistance for investigations and intelligence analysis by leveraging the NJTTF's information sharing and access to unique information related to possible threats. Supported units do this by submitting request for information to the NJTTF. The NJTTF TFOs, in answering RFIs, coordinate to provide a collaborative response that includes name checks and searches for terrorism-related information (i.e. groups and organizations associations, events,

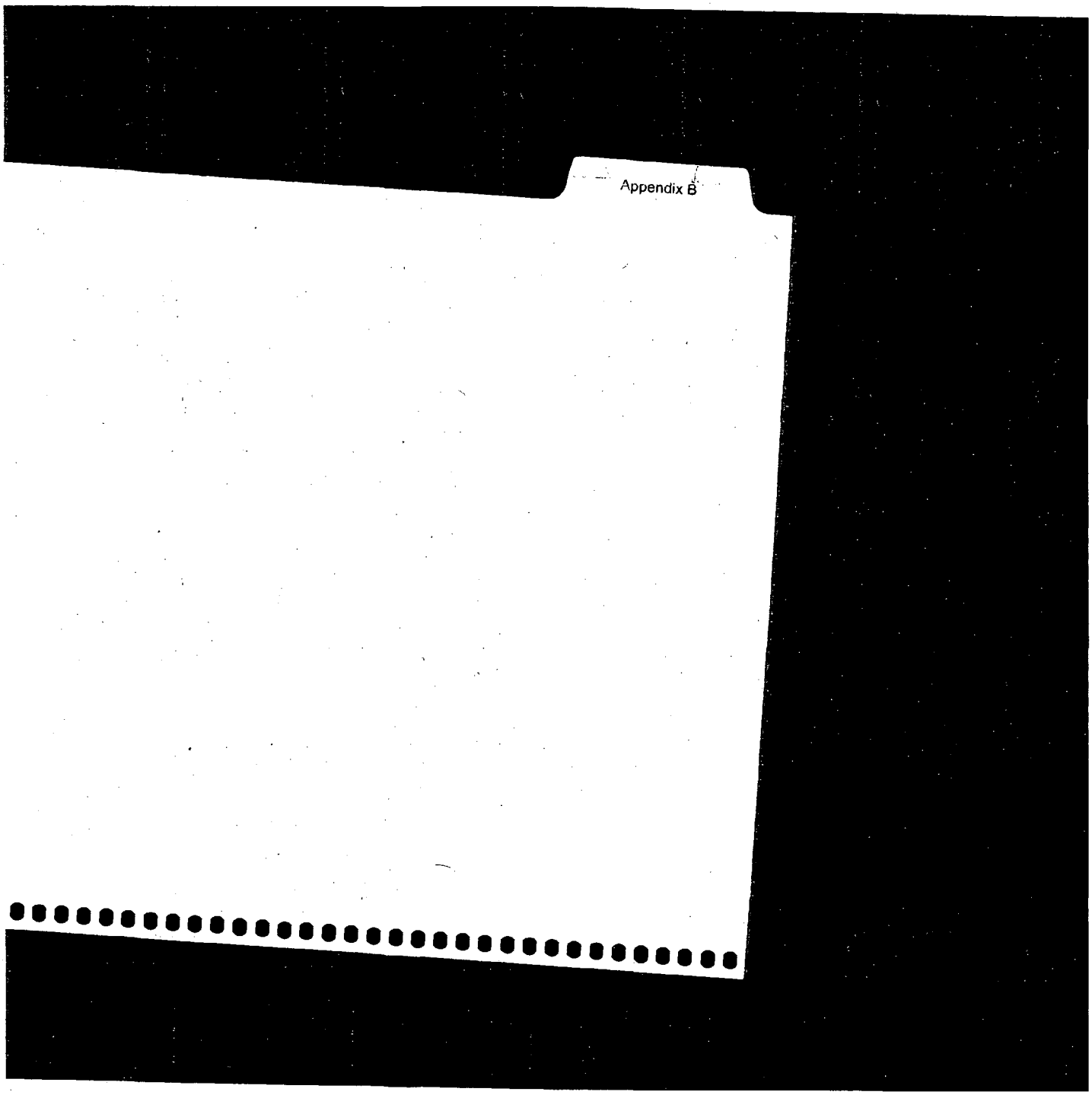
facilities, special interest country travel, equipment, weapons, communication, and finances).

CTD Section and Unit Chiefs as well as SACs, and ASACs are encouraged to highlight the FBI's NJTTF existence and encourage its use to enhance ongoing investigations. The NJTTF FBI website, found at http://ctd.fbinet.fbi/njttf/, can be accessed to provide the following information:

a. JTTFs member contact information
b. NJTTF Task Force Officers' agency information
c. JTTF operation policy documents

[redacted] b7E

[redacted] b6 b7C b7E


Appendix B

To: All Field Offices From: Counterterrorism
Re: 415A-HQ-C1432188-DR, 11/24/2009

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Ensure the information contained in this communication is distributed to all personnel assigned to JTTF and/or Counterterrorism in their respective divisions.

(S):